



US006366967B1

(12) **United States Patent**
Wagner

(10) **Patent No.:** **US 6,366,967 B1**
(45) **Date of Patent:** ***Apr. 2, 2002**

(54) **OPEN NETWORK SYSTEM FOR I/O OPERATION INCLUDING A COMMON GATEWAY INTERFACE AND AN EXTENDED OPEN NETWORK PROTOCOL WITH NON-STANDARD I/O DEVICES UTILIZING DEVICE AND IDENTIFIER FOR OPERATION TO BE PERFORMED WITH DEVICE**

(75) **Inventor:** **Richard Hiers Wagner, Dunwoody, GA (US)**

(73) **Assignee:** **Datascape, Inc., Atlanta, GA (US)**

(*) **Notice:** Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) **Appl. No.:** **09/314,266**

(22) **Filed:** **May 18, 1999**

Related U.S. Application Data

(63) Continuation of application No. 08/995,123, filed on Dec. 19, 1997, now Pat. No. 5,905,908, which is a continuation of application No. 08/493,772, filed on Jun. 22, 1995, now Pat. No. 5,742,845.

(51) **Int. Cl.⁷** **G06F 13/14**

(52) **U.S. Cl.** **710/33; 710/20; 709/227**

(58) **Field of Search** **710/1, 33, 20; 709/227**

References Cited

U.S. PATENT DOCUMENTS

4,625,276 A 11/1986 Benton et al.
4,707,592 A 11/1987 Ware

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

WO WO 95/16971 6/1995

OTHER PUBLICATIONS

"Europay Members Forum", Europay International, May 8, 2001, (3 pages).

(List continued on next page.)

Primary Examiner—Thomas Lee

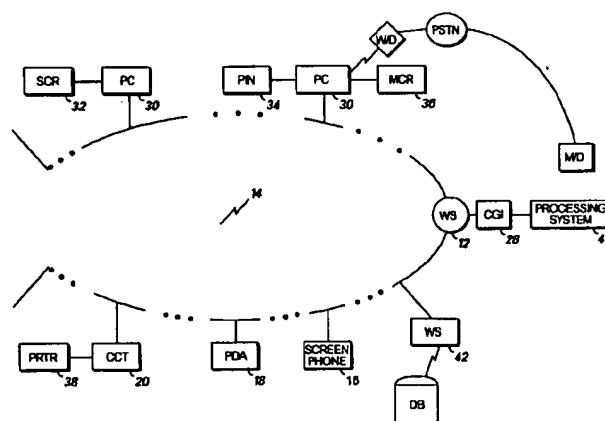
Assistant Examiner—Rehana Perveen

(74) *Attorney, Agent, or Firm*—Magainot, Addison & Moore

(57) ABSTRACT

An open network system for supporting input/output (I/O) operations for non-standard I/O devices are disclosed. The system includes a server coupled to a plurality of I/O device through an open network and an extended open system protocol that supports communication with devices that are not personal computers (PCs). These devices include magnetic stripe readers, check readers, smart card readers, credit card terminals, screen phone terminals, PIN pads, printers, and the like. The extended open network protocol includes tags which identify device and input operations and attributes which identify the location, data exchange method, and data variable names for the retrieval, acquisition, and submission of data between the server and I/O devices. Preferably, the open network protocol is implemented in a Hyper Text Transport Protocol (HTTP). Preferably, the system includes a common gateway interface (CGI) at the server which converts protocol statements communicated between the server and I/O devices to application language statements for providing data to an application program coupled to the server. Most preferably, the application statements and protocol statements are constructed in integrated statements with an editor. The editor ensures that data identifiers in the application and protocol statements are compatible. The integrated statements are then parsed by the editor to segregate the protocol statements from the application statements. The protocol statements are downloaded in a file to a client program at an I/O device for processing. The application statements are stored in a file for use by the application. In this manner, generation of the files for client and application processing are automatically done without the user ensuring the correlation of the data fields in the two files.

18 Claims, 25 Drawing Sheets



U.S. PATENT DOCUMENTS

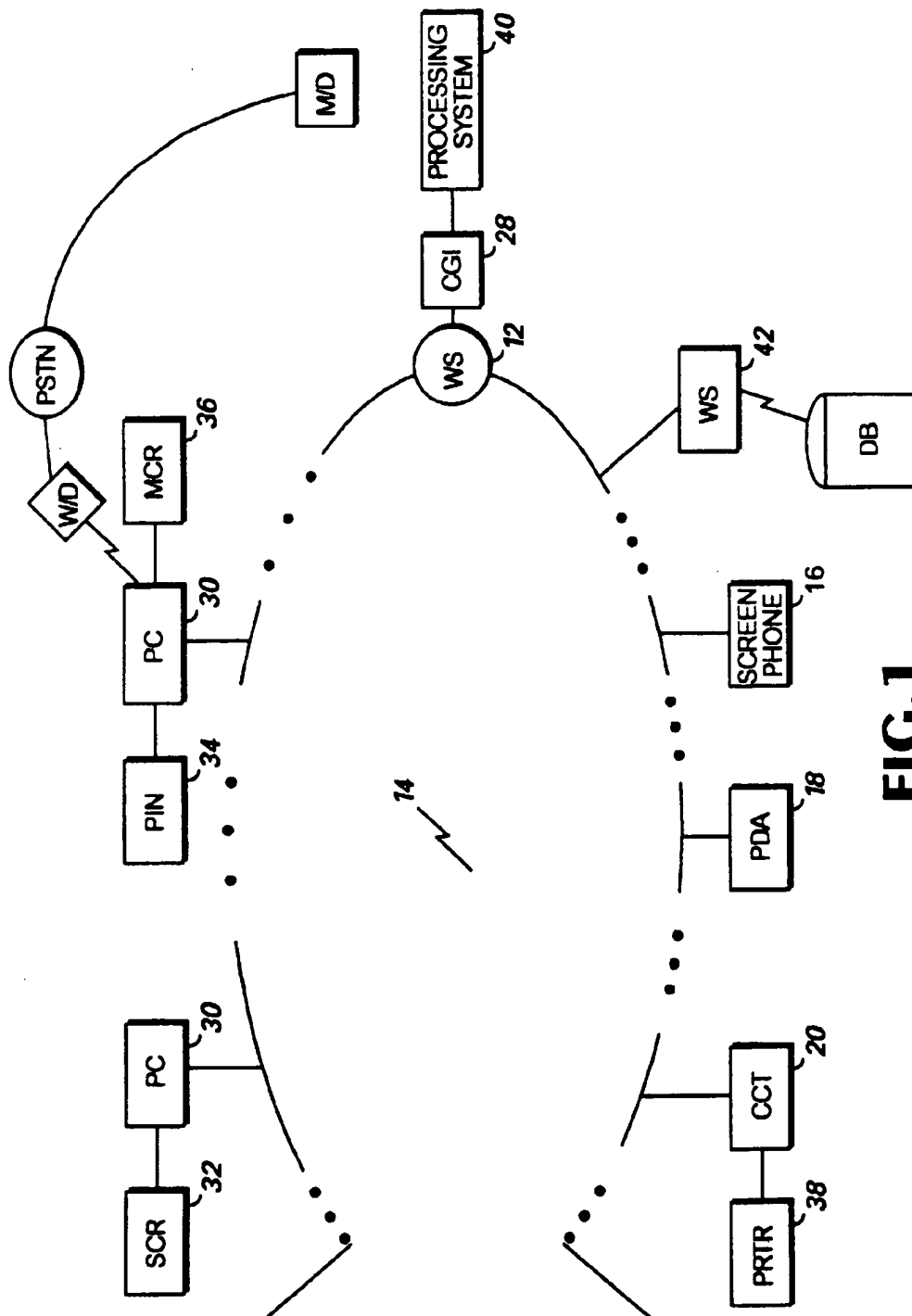
4,799,156 A 1/1989 Shavit et al.
 4,885,777 A 12/1989 Takaragi et al.
 4,962,531 A 10/1990 Sipman et al.
 4,972,463 A 11/1990 Danielson et al.
 5,018,196 A 5/1991 Takaragi et al.
 5,025,373 A 6/1991 Keyser, Jr. et al.
 5,046,094 A 9/1991 Kawamura et al.
 5,148,481 A 9/1992 Abraham et al.
 5,239,662 A 8/1993 Danielson et al.
 5,256,863 A * 10/1993 Ferguson et al. 235/383
 5,276,312 A 1/1994 McCarthy
 5,377,191 A * 12/1994 Farrell et al. 370/94.1
 5,379,344 A 1/1995 Larsson et al.
 5,386,517 A 1/1995 Sheth et al.
 5,461,217 A 10/1995 Claus
 5,475,858 A 12/1995 Bush
 5,530,844 A * 6/1996 Phillips et al. 395/500
 5,544,246 A 8/1996 Mandelbaum et al.
 5,668,878 A 9/1997 Brands
 5,732,219 A * 3/1998 Blumer et al. 395/200.57
 5,754,655 A 5/1998 Hughes et al.
 5,756,978 A 5/1998 Soltesz et al.
 5,778,067 A 7/1998 Jones et al.
 5,815,577 A 9/1998 Clark
 5,867,821 A 2/1999 Ballantyne et al.
 RE36,310 E 9/1999 Bjerrum et al.

OTHER PUBLICATIONS

- "NCR 2170 Hospitality Workstation Designed for Bars, Restaurants", AT&T New Release, Feb. 2, 1993, (2 pages).
 "AT&T to Increase Smart Card Reliability, Expand Memory to 8KB", AT&T News Release, Apr. 8, 1994, (2 pages).
 "AT&T and NCR Offer Smart Card Upgrade Kits for Bank ATMs", AT&T News Release, Nov. 17, 1993, (2 pages).
 "The Smart Card Cashes In", The Economist, Jan. 29, 1994, (2 pages).
 "NCR 7450 Terminal Brings ATM-style Interface to Point-of-Sale", AT&T News Release, Oct. 11, 1993, (4 pages).
 "Mastercard Smart Card Milestones", MasterCard International Press Office, Mar. 5, 2001, (3 pages).
 Svigals, Jerome, "Microchip Smart Cards Will Save Money", American Banker, Feb. 2, 1994, (1 page).
 Barthel, Matt, "Fears of Crime at ATMs are on the Rise", American Banker, Mar. 30, 1994, (1 page).
 "Smart Card Publication List", Smart Card Forum, Mar. 2, 2001, (7 pages).
 "Appendix: Major Electronic Purse Projects, By Country", pp. 35-50 and 52-64, Date Unknown (29 pages).
 O'Kelly, Robin, "Mondex 'Global Electronic Cash' Wins Helsinki Award", Sep. 8, 1996, (2 pages).
 "White Paper-The Euro in the Electronic Purse", Apr. 2000, (5 pages).
 "History of Gemplus", Gemplus, Mar. 2, 2001, (3 pages).
 Pauli, Ralf and Koponen, Risto, "Toward Electronic Money", Bank of Finland Bulletin, Apr. 1997, (3 pages).
 "A Frequently Asked Questions List (FAQ) for *alt.technology.smartcards*", Estonian Institute of Cybernetics, Jul. 4, 1995, (12 pages).
 Husemann, Dirk, "The Smart Card: Don't Leave Home Without It", Institute of Electrical and Electronics Engineers, Inc., Sep. 18, 2000, (9 pages).
 "Report to the Council of The European Monetary Institute on Prepaid Cards", The Working Group on EU Payment Systems, May 1994, (12 pages).
 Banerjee, Ram, "Smart Card Standards and Electronic Purse, A Review Paper", Aston University, May 1997, (20 pages).
 Townend, Robin C., "Finance: History, Development & Market Overview", The International Smart Card Industry Guide, 1995-1996, (23 pages).
 Monod, Elsbeth Marikje, "Case Study: The Multi-Functional Smart Carte Sante", The International Smart Card Industry Guide, 1995-1996, (8 pages).
 Smith, Jack "Smart Card Industry Review 1995", Smart Card Monthly Newsletter, Jan. 1996, (6 pages).
 Crotch-Harvey, Trevor, "Smart Cards in Telecoms", The International Smart Card Industry Guide, 1995-1996, (14 pages).
 Farmer, Donna and Tonnac, Remy de, "What's So Smart About Smart Cards", Gemplus, Oct. 10, 2000, (1 page).
 "P401 Definition of a pan-European IC Card", Eurescom, Mar. 5, 2001, (1 page).
 "Innovonics, Inc. Selects AMP as Manufacturer for the PC Pay Module", Innovonics News Release, May 19, 1995, (3 pages).
 Levy, Steven, "E-Money (That's What I Want)", Wired, Dec. 1994, (2 pages).
 Fickenscher, Lisa, "Banc One Gears Up to Go National With Its Microchip Smart Cards", American Banker, Jan. 27, 1994 (2 pages).
 Strachman, Daniel and Kutler, Jeffrey, "Convention Goers See Bank Future in Smart Cards", American Banker, Nov. 30, 1993, (1 page).
 Meece, Mickey, "First Data Strengthens Position in Card Processing", American Banker, Dec. 21, 1993, (1 page).
 Kutler, Jeffrey, "Prepaid Card, Even in Concept Stage, Sparking Interest Among Consumers", American Banker, Apr. 27, 1994, (1 page).
 Kutler, Jeffrey, "Visa Starts Push for Smart Card to Replace Cash", American Banker, Mar. 22, 1994, (2 pages).
 "AT&T Introduces Enhanced Multimedia Interface for ATM Networks", AT&T News Release, May 4, 1994, (2 pages).
 "Trendar and AT&T Test Contactless Smart Cards at Truck Stops", AT&T News Release, Feb. 26, 1993, (3 pages).
 "NCR Announces 5980 Signature Capture System for Retailers", AT&T News Release, Sep. 30, 1991, (2 pages).
 Merckling, Roger and Anderson, Anne "Smart Card Introduction", Mar. 1994, (16 pages).
 Merckling, Roger and Anderson, Anne, "DCE Smart Card Integration", Mar. 1994, (16 pages).
 "Chapter 2-Technology", Smart Card Primer, The Schuler Consultancy, ©1993, pp. 13-24 and 26-29, (16 pages).
 "CP8® PRODUCTS, PASCAM, Network Security Processor", Jan. 1994, (4 pages).
 "Notes on Open Networks and Device Addressing", IBM Corporation, Apr. 25, 2001, (19 pages).
 Chakrabarti, Samdih, Knight, James and Thies, Bill, "A Centralized Smart Card System Utilizing Distributed Proxies", 2000, University of Leeds, (16 pages).
 "Single-Issuer Multiple Uses", Smart Card Primer, The Schuler Consultancy, ©1993, (3 pages).
 Sazegar, Hossein, "The Impact of Smart Cards in the Global Payphone Business", Schlumberger Technologies, ©1992, (11 pages).
 Derksen, Eduard, "Money-Bit: The Open Off-Host Prepaid Card System", Ascom Autelca, Ltd., Date Unknown, (10 pages).

- Corzo, Gerardo, "Credisa's Elite Card System", Date Unknown, (5 pages).
- Cordonnier, Vincent M., "Assessing the Future of Smart Cards", Cardtech, Date Unknown, (7 pages).
- "NatWest Launch Mondex Global Electronic Cash", Smart Card News, Ltd., Dec. 1993, (7 pages).
- Merkert, Sr., Robert J., "Stored Value Cards and The Electronic Purse: Developments in the Americas", Danyl Corporation, ©1995, (8 pages).
- "CP8® Products, PinPadLINK, Readers/Encoders", Dactyl France, June 1993, (2 pages).
- "Smart Security", Byte Talk, February 1994, (2 pages).
- Verschuren, Ton, "Smart Access: Strong Authentication on the Web", Apr. 24, 2001, (10 pages).
- "PKCS #11: New Member of Public Key Cryptography", RSA Data Security, Inc., Jan. 12, 1994, (2 pages).
- Petri, Steve, "An Introduction to Smartcards", Litronic, Inc., ©1998, (2 pages).
- Violino, Bob, "The Cashless Society", Information Week, Oct. 11, 1993, (5 pages).
- Merkert, Sr., Robert J., 'Keynote Presentation for the AIC Conference, Auckland, New Zealand', Danyl Corporation, © 1995, (4 pages).
- "Videoway's Experience Shows a New Approach to the Interactive Opportunity", Inside Cable and Telecom Services, Jun. 1995, (3 pages).
- Bull CP8® News, Products and Technologies, No. 22, Oct. 1994, (2 pages).
- Bull CP8® Systems Product Sheet, Sep. 1994, (2 pages).
- "One Store's Comprehensive Loyalty Program—The Takashimaya Experience", Verifone, Inc., ©1994, (4 pages).
- "Mondex Payments Scheme", Smart Card News Ltd., Dec. 1993, (2 pages).
- "Why Consumers Are Still Carrying Cash Everywhere", Philadelphia Inquirer, Jun. 11, 1995, (2 pages).
- "Electronic Payment System Architecture for Point of Sale Application", IBM Technical Disclosure Bulletin, Jan. 1992, (1 page).
- "Portable Self Checkout Retail System", IBM Technical Disclosure Bulletin, Jun. 1992, (3 pages).
- "Transaction Completion Code Based on Digital Signatures", IBM Technical Disclosure Bulletin, Aug. 1985, (6 pages).
- "Chapter 4—Uses", Smart Card Primer, The Schuler Consultancy, ©1993, pages 57–66, 80–83, and 87–91, (19 pages).
- Figure 8.5 from p. 151 of Zoreda & Oton "Smart Cards", Artech House, ©1994, (1 page).
- "Internet Music Library Process", Date Unknown, (1 page).
- Bibliography for "CITM Working Paper WP-95-1005; Designing Electronic Catalogs for Business Value: Results from the CommerceNet Pilot", Date Unknown, (3 pages).
- Van Hove, Leo, Bibliography on Electronic Purses, Date Unknown, (4 pages).
- Bibliography for "CITM Working Paper WP-95-1006: Financial EDI Over the Internet: A Case Study", Date Unknown, (5 pages).
- Bibliography for Hawkes, P. L., Davies, Donald W., and Price W. L. "Integrated Circuit Cards, Tags, and Tokens: New Technology and Applications", Oxford: Boston: BSP Professional, ©1990, (1 page).
- Bibliography for Devargas, M., "Smart Cards and Memory Cards", Oxford; Blackwell NCC, ©1992, (1 page).
- Bibliography for Svigals, Jerome, "Smart Cards: The New Bank Cards", New York: Macmillan; London: Collier Macmillan Publishers, ©1987, (1 page).
- Bibliography for Bright, Roy, "Smart Cards: Principles, Practice, Applications", Chichester [England]: Ellis Horwood; New York: Halsted Press, ©1988, (1 page).
- Bibliography for Svigals, Jerome, "Smart Cards: The Ultimate Personal Computer", New York: Macmillan Publishing Co.; London: Collier Macmillan, ©1985, (1 page).
- Bibliography for "Applications of Computer Card Technology", Washington, D.C., U.S. Dept. of Labor, Office of the Inspector General, [1990], (1 page).
- German article entitled "Erfahrungen Mit Einer Hochsicheren, Multifunktionalen Chipkarte für Bankenanwendungen" Date Unknown, (21 pages).
- Document entitled: "Dialog Search for U.S. Patent Number 5,905,908", Date Unknown, (59 pages).
- UBI Consortium Inc. Document, Mar. 26, 2001 (2 pages).

* cited by examiner

**FIG. 1**

<u>HTML+D Attributes</u>	<u>Description</u>
<FORM ACTION = "url" FROM "file name" TO PRINTER TO "file name" FROM SCR TO SCR	To/From Web Server URL From Terminal Local File To Local Printer To Terminal Local File From Smart Card Reader To Smart Card Reader
METHOD = "GET" "POST" "PAYMENT"	Retrieve Data Store Data Directive to deliver INPUT data to a private Payment Network for authorization and settlement.
SQL <database name>	SQL statement database table

<u>Attribute</u>	<u>Value</u>	<u>Description</u>
<INPUT TYPE =	"text" "password" "checkbox" "radio" "submit" "reset"	
NAME =	<field name>	
VALUE =	<initial value>	
CHECKED =		
SIZE =		
MAXLENGTH =		
>		

<u>Attribute</u>	<u>HTML+D Value</u>	<u>Terminal Device</u>
TYPE =	"MSRT1" "MSRT2" "KEY" "PIN" "BCW" "MICR" "AMT" "INT" "LOCAL" "AUTOSUBMIT"	Mag Stripe Reader - Track 1 Mag Stripe Reader - Track 2 Terminal Command Keypad PIN Pad Bar Code Wand Check MICR Reader Dollar amount key input mask Integer key input mask Input from Local Variable Submit FORM to ACTION URL
NAME =	ip_address host_phone tid work_key datetime deposit_acct	Local Variable - Terminal's IP Address Local Variable - Local Internet Access Phone Number Local Variable - Terminal ID Local Variable - PIN encryption working key Local Variable - Date and time Local Variable - Merchant Deposit Account

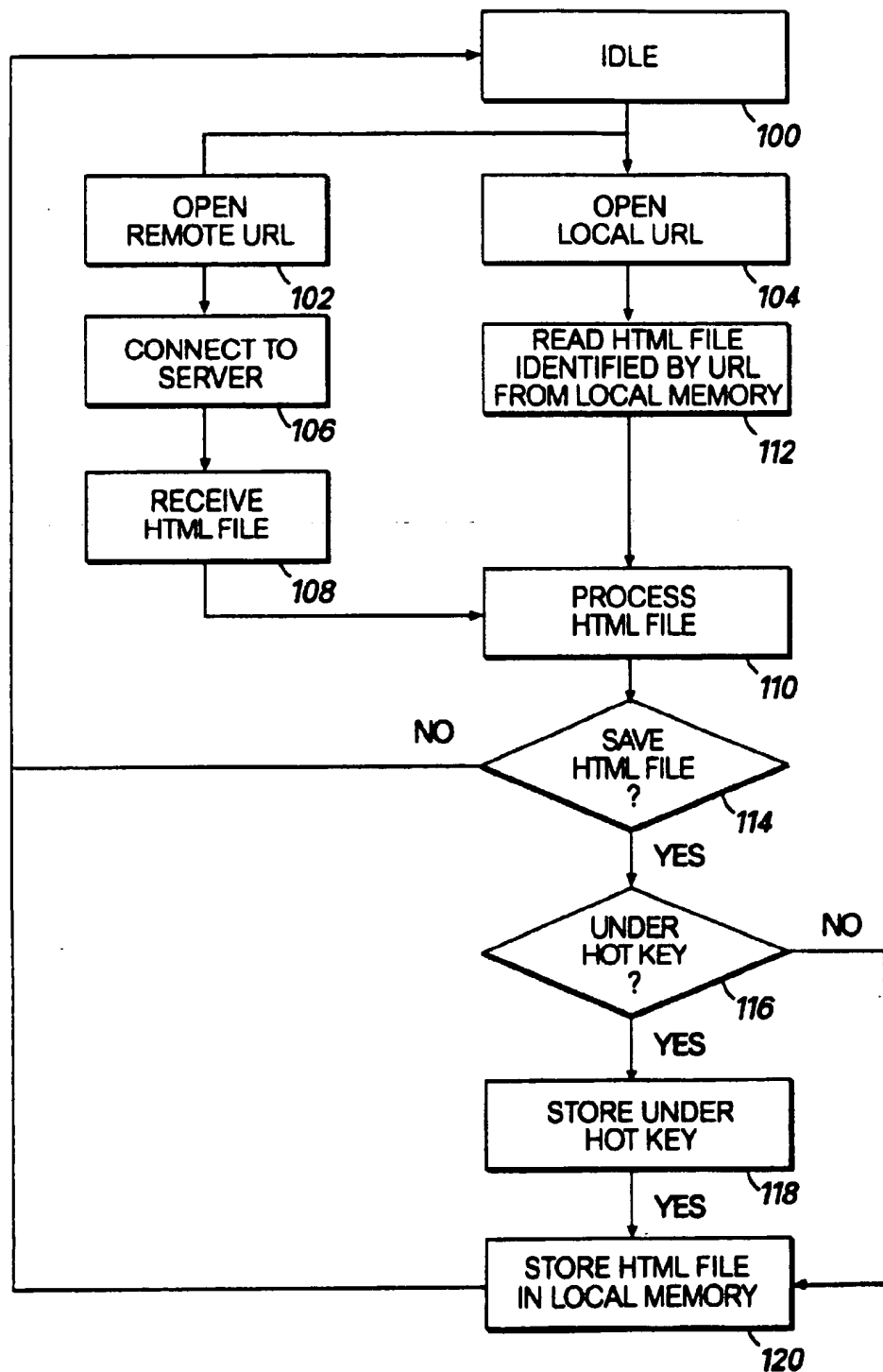
FIG.2

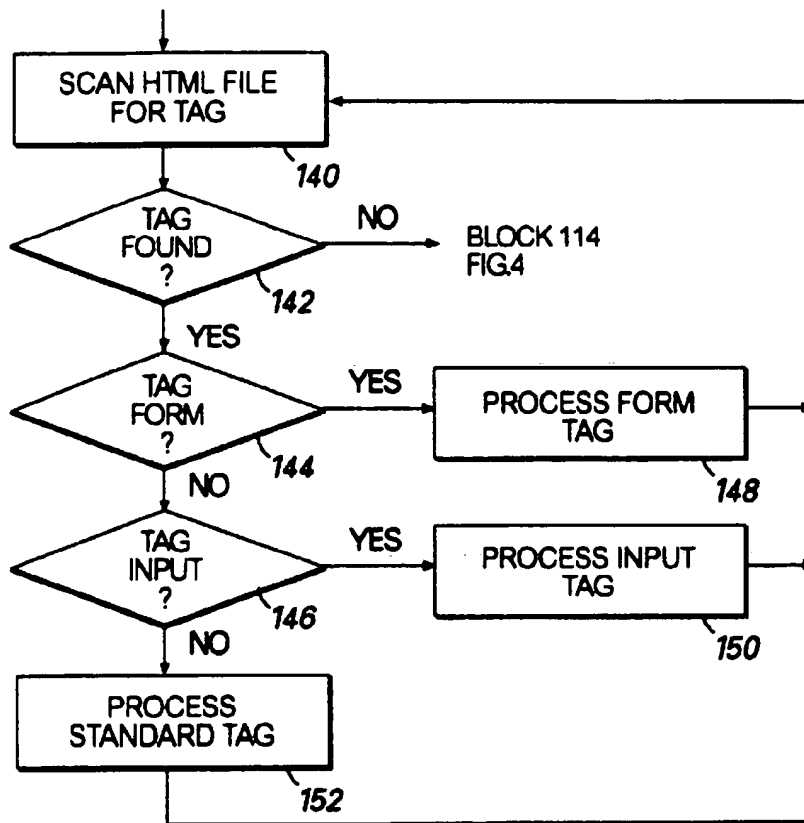
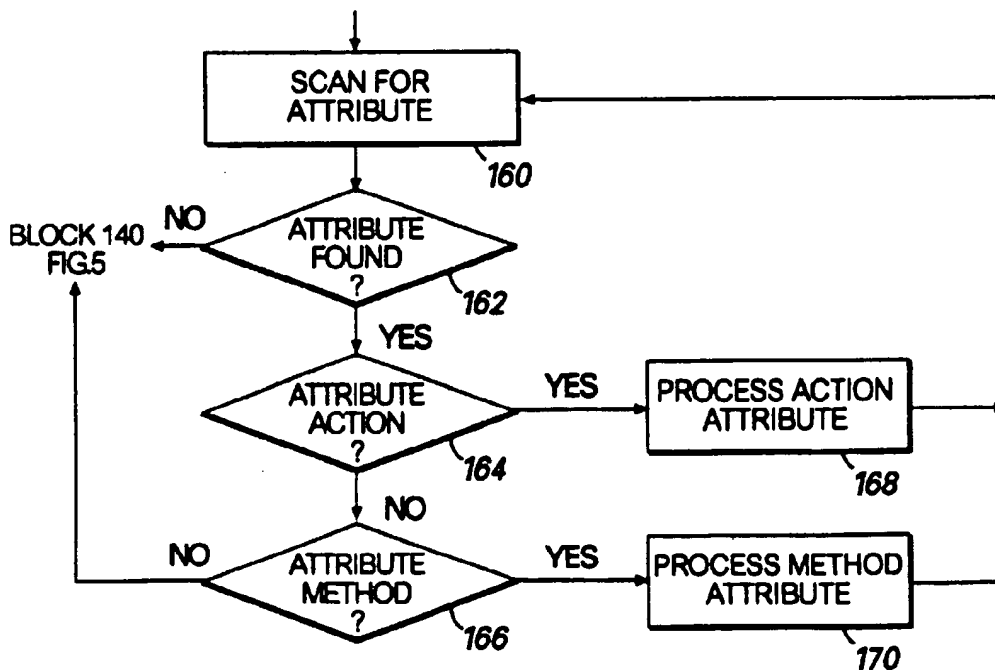
SQL Statements

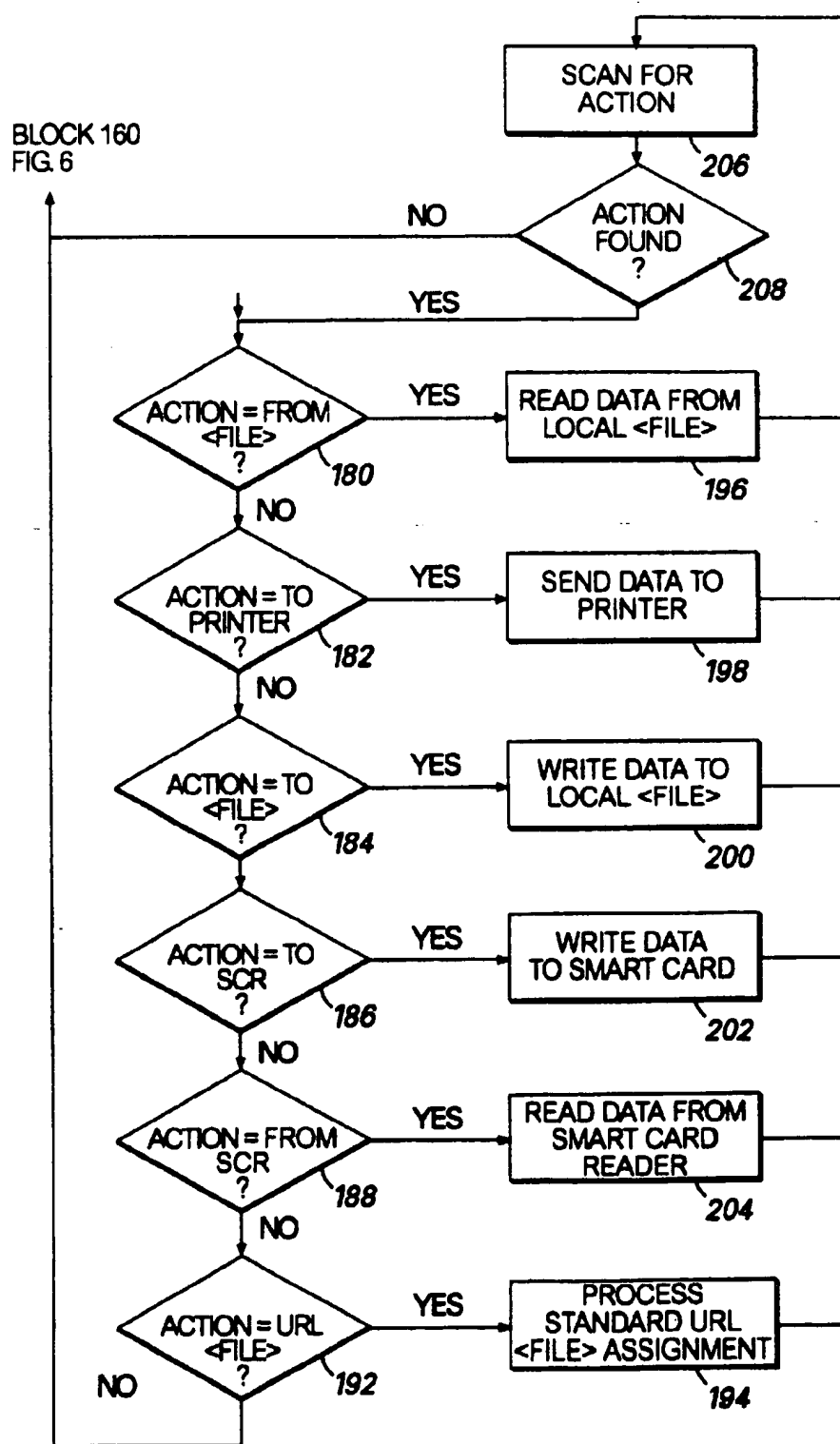
The following SQL commands represent a subset of the entire command set that varies by database vendor.

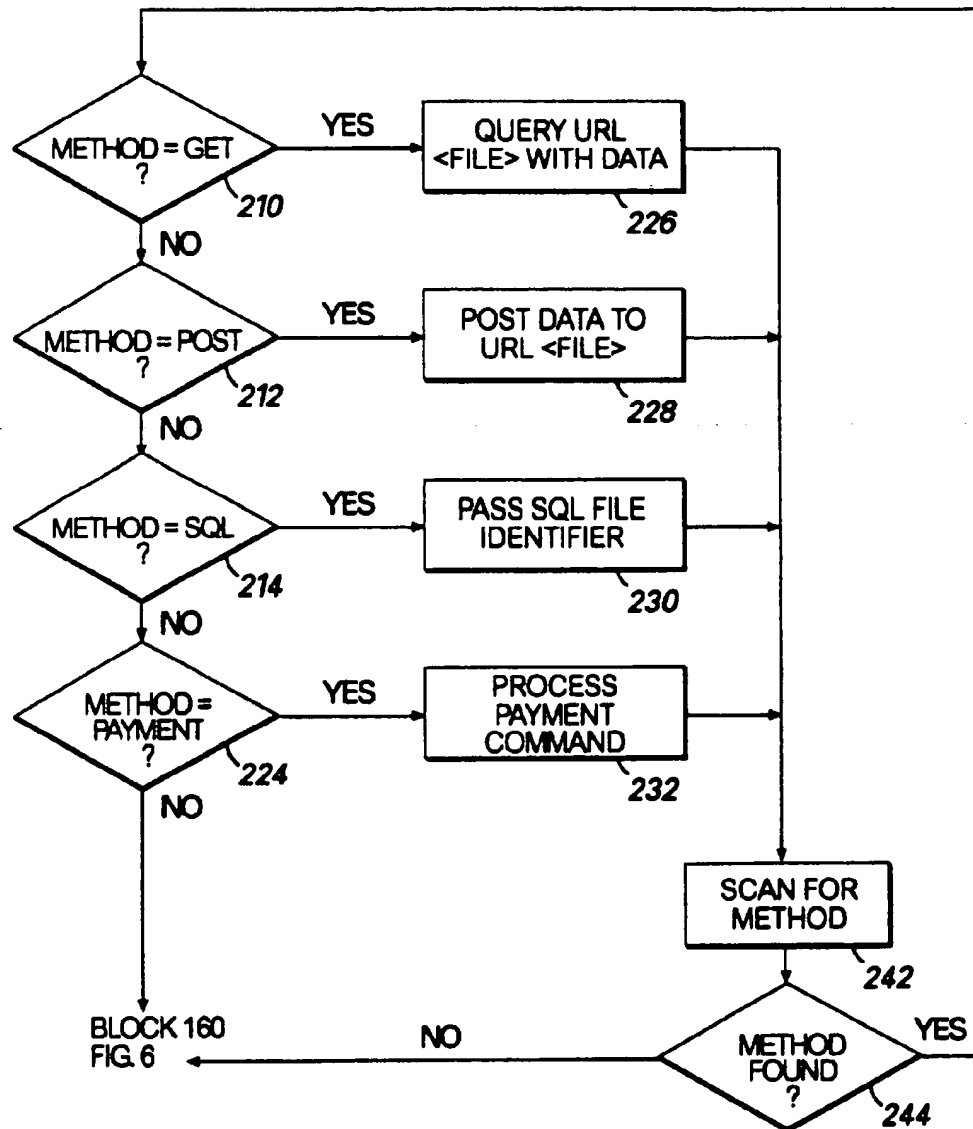
<u>HTML+D Attributes</u>	<u>Description</u>
SELECT *, field_name, ... FROM =<table name> ... WHERE =<condition> name = "constant" name LIKE "constant" name IN "constant" AND OR ORDER =ASC DESC 2 GROUP =<name>	Request field_name (one or many) from a database table Database table name Conditional selection of data Request in ascending order ...descending ...by 2's
INSERT TABLE =<table name> VALUES = "constants"	Insert new data in database table
UPDATE FROM <table name> SET =field_name = "constant" [WHERE =<condition>]	Update field_name in database table Update if WHERE clause is satisfied
DELETE FROM <table name> [WHERE =<condition>]	Delete all columns that satisfy WHERE clause
CREATE TABLE <table_name> PRIMARY KEY <name>	Create database table

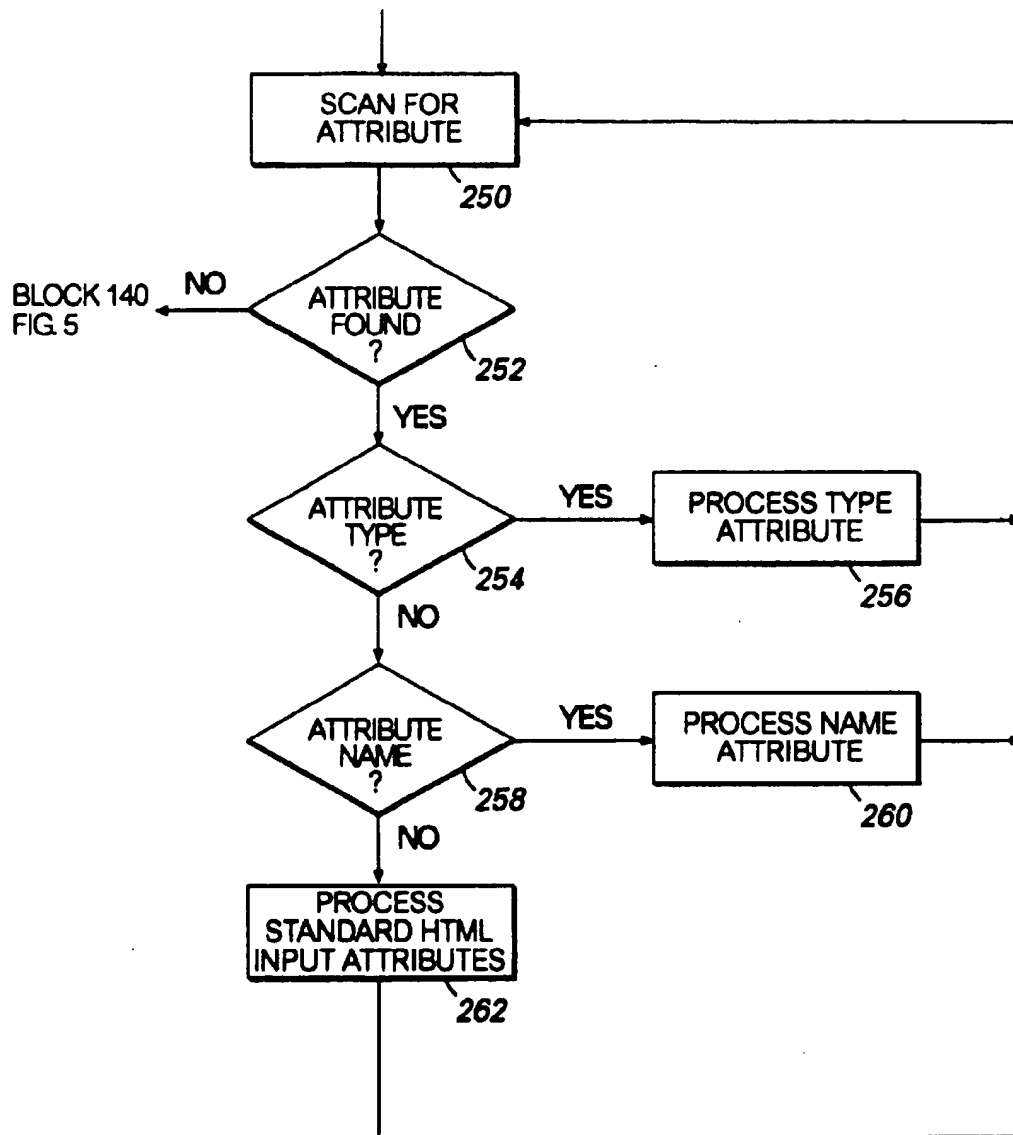
FIG. 3

**FIG. 4**

**FIG. 5****FIG. 6**

**FIG. 7**

**FIG. 8**

**FIG. 9**

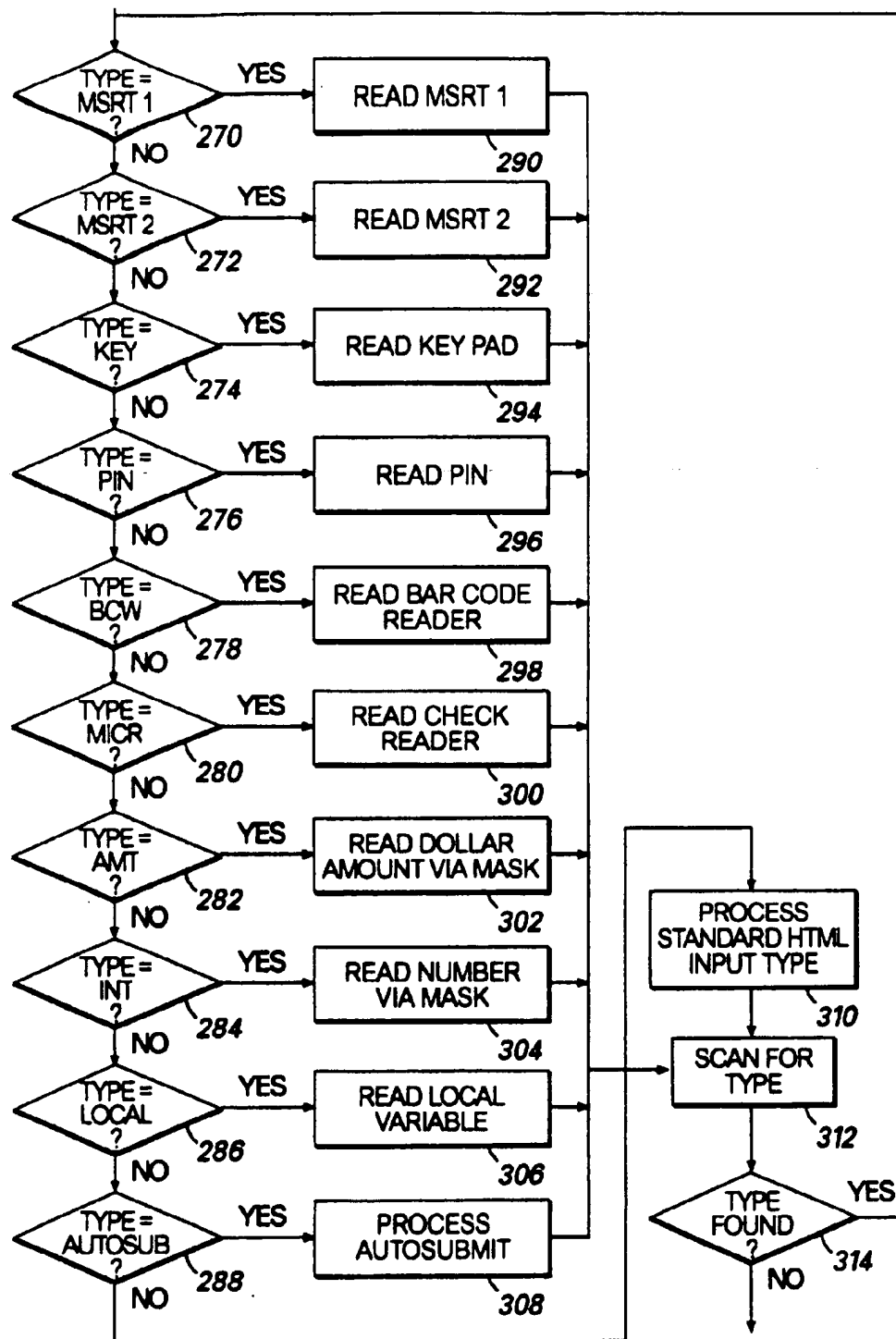
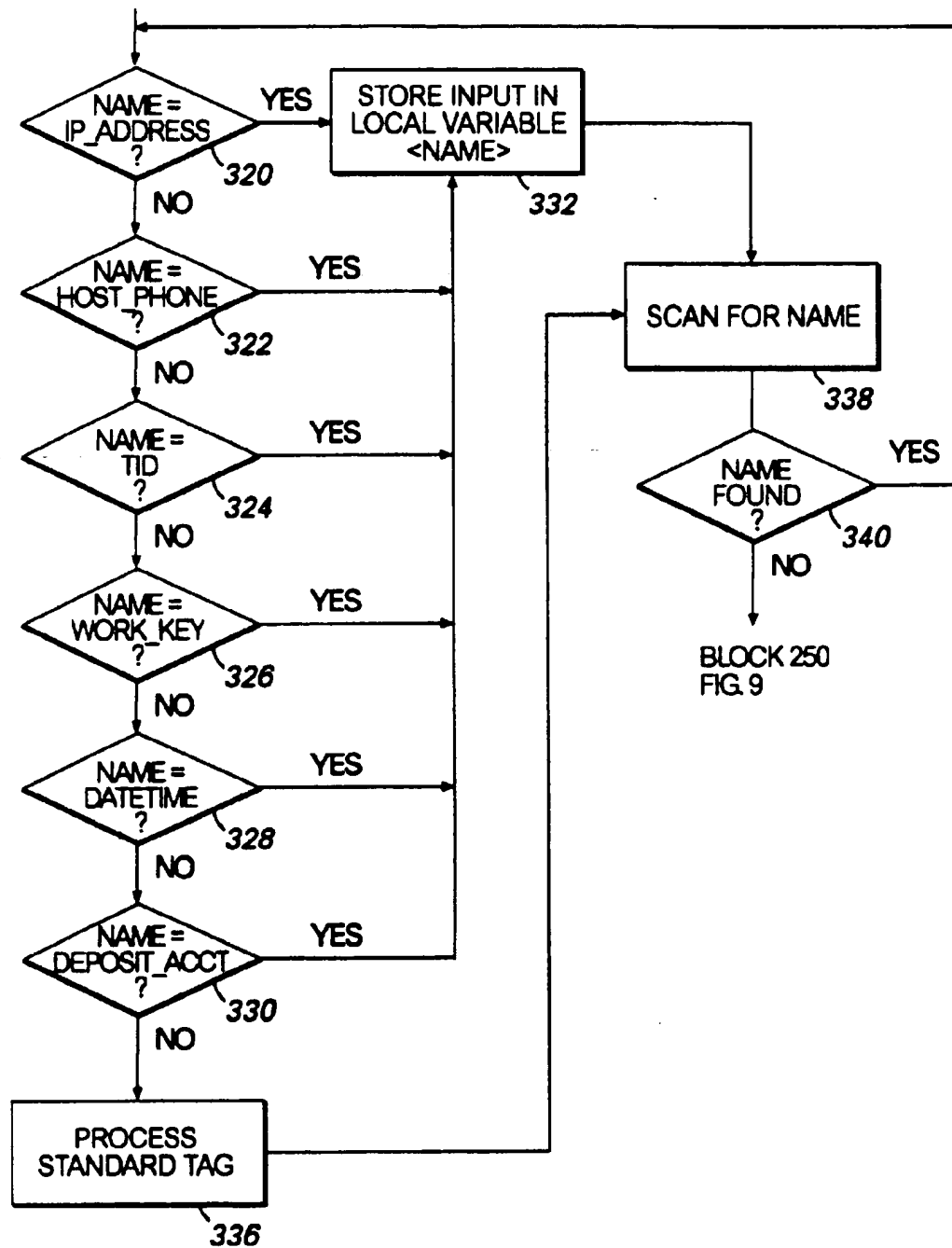
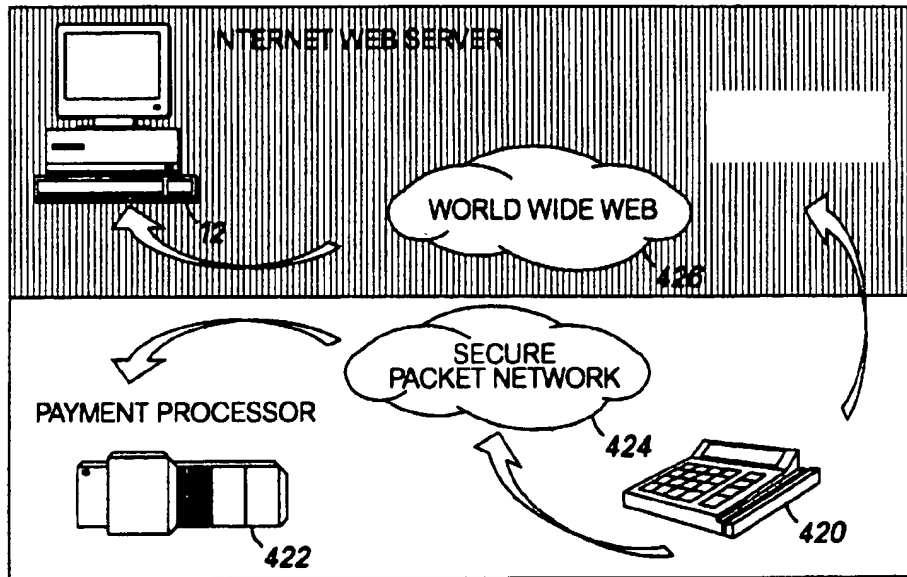
BLOCK 250
FIG. 9

FIG.10

**FIG.11**

1. <FORM ACTION=URL METHOD= GET>
2. <FORM ACTION=URL METHOD= POST>
3. <FORM ACTION=URL METHOD= SQL <database_name>

FIG.12**FIG.13A**

```
<FORM ACTION=<filename> METHOD=PAYMENT>
<INPUT TYPE=AUTOSUBMIT>
</FORM>
```

FIG.13B

```
<FORM ACTION=dsinet METHOD=PAYMENT>
<INPUT TYPE=LOCAL NAME=DEPOSIT_ACCT VALUE=123456890234567890>
<INPUT TYPE=AUTOSUBMIT>
</FORM>
```

FIG.13C

1.a. Transaction Request HTML+D

500

```

<HTML>
<BODY>
<FORM ACTION=dbase_URL
      METHOD=SQL
      "BEGIN TRAN
      IF NOT EXISTS ( SELECT substring(account, 1, 20) FROM auth_table)
      BEGIN
      INSERT TABLE=log_table VALUES=(getdate(),tid, substring (account, 1,20) ,
      substring( account, 22, 4), amount)
      SELECT * FROM log_table WHERE trandate = getdate()
      END
      ELSE SELECT * FROM error_table WHERE error_no=1
      COMMIT TRAN">
<INPUT TYPE="LOCAL" NAME=tid>
ENTER ACCOUNT NUMBER:
<INPUT TYPE="MSRT2" SIZE=40 NAME=account>
ENTER AMOUNT
<INPUT TYPE="AMT" SIZE=8 NAME=amount>
<INPUT TYPE="AUTOSUBMIT">
</FORM>
</BODY>
</HTML>

```

1.b. Transaction Accepted Response

510

```

<HTML>
<BODY>
<FORM ACTION=TO PRINTER METHOD=POST>
JUNE 1 1995      10:30AM      PURCHASE</P>
TERMINAL ID:      999999999</P>
ACCOUNT NUMBER      99999999999999999999</P>
EXP DATE:      99/99</P>
AMOUNT      $9999.99</P>
AUTH NUMBER      999999999</P>
</p>
-----</p>
      CUSTOMER SIGNATURE </p>
</FORM>
APPROVED:999999999</P>
</BODY>
</HTML>

```

1.c. Transaction Declined or Submit Error Response

520

```

<HTML>
<BODY>
DECLINED<MESSAGE>
</BODY>
</HTML>

```

FIG.14

2.a. Transaction Request HTML+D

550

```

<HTML>
<BODY>
<FORM ACTION=dbase URL
METHOD=SQL"BEGIN TRAN
  IF NOT EXISTS ( SELECT substring(account, 1, 20) FROM auth_table)
  BEGIN
    INSERT TABLE=log_table VALUES=(getdate(),tid, substring( account, 1,20),
    substring( account, 22, 4), amount)
  END
  ELSE BEGIN
    SELECT * FROM error_table WHERE error_no=1
    RETURN
  END
  INSERT TABLE=order_table VALUES=( getdate(), cust_name,address,city, state, zip,
  part_code, unit_price, tax, ship_method, ship_chrg, unit_price + tax +
  ship_chrg, substring( account, 1, 20) ,substring( account, 22, 4))
  SELECT * FROM order_table WHERE trandate = getdate()
  COMMIT TRAN">
CUSTOMER NAME:
<INPUT TYPE="TEXT" SIZE=30 NAME=cust_name></p>
ADDRESS:
<INPUT TYPE="TEXT" SIZE=40 NAME=address></p>
CITY:
<INPUT TYPE="TEXT" SIZE=20 NAME=city></p>
STATE:
<INPUT TYPE="TEXT" SIZE=2 NAME=state>
ZIP:
<INPUT TYPE="TEXT" SIZE=10 NAME=address></p>
SCAN PART CODE:
<INPUT TYPE="BCW" SIZE=9 NAME=part_code></p>
ENTER UNIT PRICE:
<INPUT TYPE="AMT" SIZE=8 NAME=unit_price></p>
TAX:
<INPUT TYPE="AMT" SIZE=5 NAME=tax></p>
SHIPPING METHOD:
<INPUT TYPE="TEXT" SIZE=10 NAME=ship_method></p>
SHIPPING AMOUNT:
<INPUT TYPE="AMT" SIZE=5 NAME=ship_chrg></p>
SLIDE CARD:
<INPUT TYPE="MSRT2" SIZE=40 NAME=account></p>
<INPUT TYPE="SUBMIT" >
</FORM>
</BODY>
</HTML>

```

FIG.15A

2.b. Transaction Accepted Response

555

```
<HTML>
<BODY>
<FORM ACTION=TO PRINTER METHOD=POST>
ORDER # 9999999999 APPROVED</p>
JUNE 1 1995      10:30AM      PURCHASE</P>
TERMINAL ID:      99999999</P>
NAME: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</p>
ADDRESS:</p>
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</p>
CITY: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</p>
STATE: XX      ZIP: XXXXXXXXXX</p>
ACCOUNT NUMBER: 999999999999999999</p>
EXP DATE:      99/99</p>
PART CODE:      99999999</p>
UNIT PRICE:      $9999.99</p>
SHIP METHOD: XXXXXXXX CHARGE      $9999.99</p>
TOTAL AMOUNT:      $9999.99</p>
AUTH NUMBER:      99999999</p>
</p>

-----</p>
      CUSTOMER SIGNATURE</p>

</FORM>
</BODY>
</HTML>
```

2.c. Transaction Declined or Submit Error Response

560

```
<HTML>
<BODY>
DECLINED <error code>
</BODY>
</HTML>
```

FIG. 15B

3.a. Transaction Request HTML+D

```
<HTML>
<BODY>
<FORM ACTION=dbase_URL
METHOD SQL
  "INSERT TABLE=order_table VALUES=( getdate(), cust_name,address,city, state, zip,
    part_code, unit_price, tax, ship_method, ship_chrg,unit_price + tax +
    ship_chrg, substring( account, 1, 20) ,substring( account, 22, 4))
  SELECT * FROM order_table WHERE trandate = getdate()">
<INPUT TYPE="LOCAL" NAME=tid>
CUSTOMER NAME:
<INPUT TYPE="TEXT" SIZE=30 NAME=cust_name></p>
ADDRESS:
<INPUT TYPE="TEXT" SIZE=40 NAME=address></p>
CITY:
<INPUT TYPE="TEXT" SIZE=20 NAME=city></p>
STATE:
<INPUT TYPE="TEXT" SIZE=2 NAME=state>
ZIP:
<INPUT TYPE="TEXT" SIZE=10 NAME=address></p>
ENTER PART CODE:
<INPUT TYPE="TEXT" SIZE=10 NAME=part_code></p>
ENTER UNIT PRICE:
<INPUT TYPE="AMT" SIZE=8 NAME=unit_price></p>
TAX:
<INPUT TYPE="AMT" SIZE=5 NAME=tax></p>
SHIPPING METHOD:
<INPUT TYPE="TEXT" SIZE=10 NAME=ship_method></p>
SHIPPING AMOUNT:
<INPUT TYPE="AMT" SIZE=5 NAME=ship_chrg></p>
<INPUT TYPE="SUBMIT" >
</FORM>
</BODY>
</HTML>
```

FIG.16A

3.b. Transaction Accepted Response

```
<HTML>
<BODY>
<FORM ACTION=TO PRINTER METHOD=POST>
ORDER # 9999999999 APPROVED</p>
JUNE 1 1995      10:30AM      PURCHASE</P>
TERMINAL ID:      999999999</P>
NAME: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</p>
ADDRESS:</p>
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</p>
CITY: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</p>
STATE: XX      ZIP:XXXXXXXXXXXXX</p>
PART CODE:      999999999</p>
UNIT PRICE:      $9999.99</p>
SHIP METHOD:XXXXXXX CHARGE:      $9999.99</p>
TOTAL AMOUNT:      $9999.99</p>
</FORM>
<FORM ACTION=<file_name> METHOD=PAYMENT>
<INPUT TYPE=AUTOSUBMIT>
</FORM>
</BODY>
</HTML>
```

3.c. Transaction Declined or Submit Error Response

```
<HTML>
<BODY>
DECLINED <error code>
</BODY>
</HTML>
```

FIG.16B

4.a. Transaction Request HTML+D

```
<HTML>
<BODY>
<FORM ACTION=SCR1 METHOD=POST>
<INPUT TYPE="LOCAL" NAME=tid>
SLIDE CARD:
<INPUT TYPE="MSRT2" SIZE=40 NAME=track2>
ENTER AMOUNT:
<INPUT TYPE="AMT" SIZE=8 NAME=amount>
<INPUT TYPE="LOCAL" NAME=work_key>
<INPUT TYPE="AUTOSUBMIT">
</FORM>
</BODY>
</HTML>
```

4.b. Transaction Accepted HTML+D

```
<HTML>
<BODY>
<FORM ACTION=TO PRINTER METHOD=POST>
DATE:99/99/99                                TIME:9999A</P>
ACCOUNT NUMBER    999999999999999999999999</p>
EXP DATE:                                                99/99</p>
AMOUNT:                                                  $9999.99</p>
AUTH NUMBER                                             9999999999</p>
</FORM>
APPROVED:9999999999</P>
</BODY>
</HTML>
```

4.c. Transaction Declined or Submit Error Response

```
<HTML>
<BODY>
DECLINED <error code>
</BODY>
</HTML>
```

FIG. 17A

5.a. Transaction Request HTML+D

```
<HTML>
<BODY>
<FORM ACTION=SCR2 METHOD=POST>
<INPUT TYPE="LOCAL" NAME=tid>
ENTER PIN:
<INPUT TYPE="PASSWORD" SIZE=4 NAME=pin>
ENTER AMOUNT:
<INPUT TYPE="AMT" SIZE=8 NAME=amount>
<INPUT TYPE="LOCAL" NAME=work_key>
<INPUT TYPE="AUTOSUBMIT">
</FORM>
</BODY>
</HTML>
```

5.b. Transaction Accepted HTML+D

```
<HTML>
<BODY>
<FORM ACTION=TO PRINTER METHOD=POST>
DATE:99/99/99 TIME:9999A</P>
ACCOUNT NUMBER 99999999999999999999</P>
EXP DATE: 99/99</P>
AMOUNT $9999.99</P>
AUTH NUMBER 99999999</P>
</FORM>
APPROVED:9999999999</P>
</BODY>
</HTML>
```

5.c. Transaction Declined or Submit Error Response

```
<HTML>
<BODY>
DECLINED <error code>
</BODY>
</HTML>
```

FIG.17B

6.a Transaction Request HTML+D

```
<HTML>
<BODY>
<FORM ACTION=host_URL METHOD=POST>
<INPUT TYPE="LOCAL" NAME=tid>
SLIDE CARD
<INPUT TYPE="MSRT2" SIZE=40 NAME=track2>
<INPUT TYPE="PIN" SIZE=4 NAME=pin>
ENTER AMOUNT:
<INPUT TYPE="AMT" SIZE=8 NAME=amount>
<INPUT TYPE="AUTOSUBMIT">
</FORM>
</BODY>
</HTML>
```

6.b. Transaction Accepted HTML+D

```
<HTML>
<BODY>
<FORM ACTION=TO PRINTER METHOD=POST>
DATE:99/99/99                                TIME:9999A</P>
TERMINAL ID:                                999999999</P>
ACCOUNT NUMBER    999999999999999999999999</P>
EXP DATE:                                                99/99</P>
AMOUNT                $9999.99</P>
AUTH NUMBER          999999999</P>
</FORM>
APPROVED:9999999999</P>
</BODY>
</HTML>
```

6.c. Transaction Declined or Submit Error Response

```
<HTML>
<BODY>
DECLINED <error code>
<INPUT TYPE="LOCAL" NAME=work_key VALUE="9999999999999999">
</BODY>
</HTML>
```

FIG. 18

7.a. Transaction Request HTML+D

```
<HTML>
<BODY>
<FORM ACTION=dbase_URL
      METHOD=SQL
      "IF EXISTS ( SELECT account FROM check_table)
        SELECT * FROM check_table WHERE account = DDAaccount
      ELSE SELECT * FROM error_table WHERE error_no=1">
<INPUT TYPE="LOCAL" NAME=tid>
SCAN CHECK:
<INPUT TYPE="MICR" SIZE=20 NAME=account>
ENTER AMOUNT
<INPUT TYPE="AMT" SIZE=8 NAME=amount>
<INPUT TYPE="AUTOSUBMIT">
</FORM>
</BODY>
</HTML>
```

7.b. Transaction Accepted Response

```
<HTML>
<BODY>
<FORM ACTION=TO PRINTER METHOD=POST>
DATE:99/99/99                                TIME:9999</P>
TERMINAL ID:                                999999999</P>
ACCOUNT NUMBER    9999999999999999999999</P>
AMOUNT                                $9999.99</P>
AUTH NUMBER                                999999999</P>
</FORM>
APPROVED:9999999999</P>
</BODY>
</HTML>
```

7.c. Transaction Declined or Submit Error Response

```
<HTML>
<BODY>
DECLINED <error code>
</BODY>
</HTML>
```

FIG. 19

8.a. Transaction Request HTML+D

```

<HTML>
<BODY>
<FORM ACTION=dbase_URL
METHOD=SQL
*BEGIN TRAN
IF NOT EXISTS ( SELECT substring(account,51,20) FROM auth_table)
BEGIN
SELECT cur_bal FROM cust_tbl WHERE substring(account,51,20)=account
SELECT amount=amount-( points / .01 )
SELECT cur_bal=cur_bal + ( amount * .01 )
UPDATE TABLE=cust_tbl VALUES=( getdate(), account, cur_bal - points )
SELECT * FROM log_table WHERE transdate = getdate()
INSERT TABLE=log_table VALUES=( getdate(), tid, substring(account,51,20),
substring( account, 72, 4), amount)
END
ELSE SELECT * FROM error_table WHERE error_no=1"
COMMIT TRAN">
<INPUT TYPE="LOCAL" NAME=tid>
ENTER ACCOUNT NUMBER:
<INPUT TYPE="MSRT1" SIZE=90 NAME=account>
ENTER AMOUNT
<INPUT TYPE="AMT" SIZE=8 NAME=amount>
REDEEM POINTS?
<INPUT TYPE="INT" SIZE=6 NAME=points>
<INPUT TYPE="AUTOSUBMIT">
</FORM>
</BODY>
</HTML>

```

8.b. Transaction Accepted Response

```

<HTML>
<BODY>
<FORM ACTION=TO PRINTER METHOD=POST>
JUNE 1 1995      10:30AM      PURCHASE</P>
TERMINAL ID:      999999999</P>
ACCOUNT NUMBER    99999999999999999999</P>
EXP DATE          99/99</P>
AMOUNT            $9999.99</P>
AUTH NUMBER       99999999</P>
</p>
-----</p>
CUSTOMER SIGNATURE</p>
</p>
THANK YOU!!</p>
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</p>
POINTS REDEEMED:      999999</p>
POINTS EARNED:        999999</p>
CURRENT POINT BALANCE 999999</p>
</FORM>
APPROVED:999999999</P>
</BODY>
</HTML>

```

8.c. Transaction Declined or Submit Error Response

```

<HTML>
<BODY>
DECLINED <MESSAGE>
</BODY>
</HTML>

```

FIG.20

9.a. Transaction Request HTML+D

```

<HTML>
<BODY>
<FORM ACTION=dbase_URL
      METHOD=SQL
      "SELECT fields FROM table WHERE condition">
<INPUT TYPE="LOCAL" NAME=tid>
ENTER SEARCH TABLE NAME:
<INPUT TYPE="TEXT" SIZE=10 NAME=table>
ENTER SEARCH FIELD NAMES:
<INPUT TYPE="TEXT" SIZE=100 NAME=fields>
ENTER SEARCH CONDITION:
<INPUT TYPE="TEXT" SIZE=50 NAME=condition>
<INPUT TYPE="AUTOSUBMIT">
</FORM>
</BODY>
</HTML>

```

9.b. Transaction Response

```

<HTML>
<BODY>
<FORM ACTION=TO PRINTER METHOD=POST>
FIELD1  FIELD2  FIELD3  .....  FIELDN  </p>
-----
XXXXX  XXXXX  XXXXX  XXXXX  XXXXX  </p>
XXXXX  XXXXX  XXXXX  XXXXX  XXXXX  </p>
.
.
XXXXX  XXXXX  XXXXX  XXXXX  XXXXX  </p>
</FORM>
</BODY>
</HTML>

```

FIG.21

10.a. Transaction Request HTML+D

```
<HTML>
<BODY>
<FORM ACTION=dbase_URL
      METHOD=SQL
      * INSERT TABLE=log_table VALUES=( getdate(), tid, gross_sales, opn_chks, voids,
      emp_disc, mgr_disc, vip_card, man_over, coupons, sales_tax, c_dep1, c_dep2,
      c_dep3, c_dep4, chg_fund, cc_dep, batch_no, chrg_sales, paid_outs, co_sales,
      cc_sales, te_sales, gross_sales - opn_chks - voids - emp_disc - mgr_disc - vip_card -
      man_over - coupons - sales_tax, gross_sales - opn_chks - voids -
      emp_disc - mgr_disc - vip_card - man_over - coupons - c_dep1 - c_dep2 -
      c_dep3 - c_dep4 - chg_fund - cc_dep - batch_no - chrg_sales - paid_outs)
      SELECT * FROM log_table WHERE trandate = getdate())">
<INPUT TYPE="LOCAL" NAME=tid>
ENTER GROSS SALES:
<INPUT TYPE="AMT" SIZE=8 NAME=gross_sales>
ENTER OPEN CHECKS:
<INPUT TYPE="INT" SIZE=7 NAME=opn_chks>
ENTER VOIDS:
<INPUT TYPE="INT" SIZE=7 NAME=voids>
ENTER EMP DISCOUNTS:
<INPUT TYPE="INT" SIZE=7 NAME=emp_disc>
ENTER MGR DISCOUNT:
<INPUT TYPE="INT" SIZE=7 NAME=mgr_disc>
ENTER VIP CARD:
<INPUT TYPE="INT" SIZE=7 NAME=vip_card>
ENTER MANUAL OVERRINGS:
<INPUT TYPE="INT" SIZE=7 NAME=man_over>
ENTER COUPONS:
<INPUT TYPE="INT" SIZE=7 NAME=coupons>
ENTER SALES TAX:
<INPUT TYPE="AMT" SIZE=8 NAME=sales_tax>
ENTER CASH DEPOSIT 1:
<INPUT TYPE="AMT" SIZE=8 NAME=c_dep1>
ENTER CASH DEPOSIT 2:
<INPUT TYPE="AMT" SIZE=8 NAME=c_dep2>
ENTER CASH DEPOSIT 3:
<INPUT TYPE="AMT" SIZE=8 NAME=c_dep3>
ENTER CASH DEPOSIT 4:
<INPUT TYPE="AMT" SIZE=8 NAME=c_dep4>
ENTER CHANGE FUND:
<INPUT TYPE="AMT" SIZE=8 NAME=chg_fund>
```

FIG.22A

```
ENTER CC DEPOSIT:
<INPUT TYPE="AMT" SIZE=8 NAME=cc_dep>
ENTER BATCH #:
<INPUT TYPE="INT" SIZE=3 NAME=batch_no>
ENTER CHARGE SALES:
<INPUT TYPE="AMT" SIZE=8 NAME=chrg_sales>
ENTER PAID OUTS:
<INPUT TYPE="INT" SIZE=8 NAME=paid_outs>
ENTER CARRY OUT SALES:
<INPUT TYPE="AMT" SIZE=8 NAME=co_sales>
ENTER CREDIT CARD SALES:
<INPUT TYPE="AMT" SIZE=8 NAME=cc_sales>
ENTER TAX EXEMPT SALES:
<INPUT TYPE="AMT" SIZE=8 NAME=te_sales>
<INPUT TYPE="AUTOSUBMIT">
</FORM>
</BODY>
</HTML>
```

10.b. Transaction Response

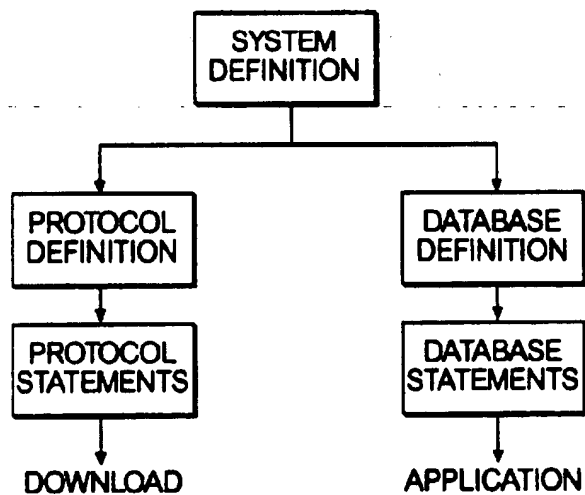
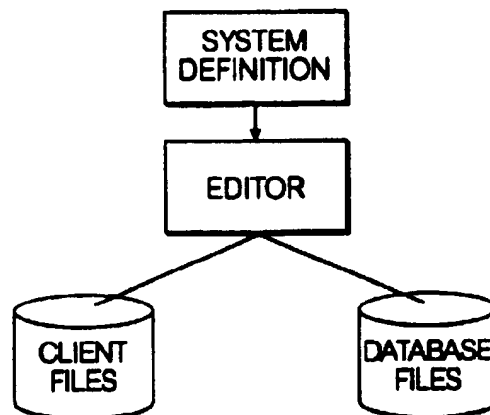
```
<HTML>
<BODY>
<FORM ACTION=TO PRINTER METHOD=POST>
JUNE 1 1995      10:30AM      DAILY REPORT</P>
TERMINAL ID:    99999999</P>
GROSS SALES    999999.99</P>
VOIDS          99      99999.99</P>
EMP DISCOUNTS 99      99999.99</P>
MANAGER DISCOUNTS 99      99999.99</P>
VIP CARD       99      99999.99</P>
COUPONS        99      99999.99</P>
MANUAL OVERRINGS 99      99999.99</P>
SALES TAX      999999.99</P>
CASH DEPOSIT 1 999999.99</P>
CASH DEPOSIT 2 999999.99</P>
CASH DEPOSIT 3 999999.99</P>
CASH DEPOSIT 4 999999.99</P>
CASH DEPOSIT 5 999999.99</P>
CHANGE FUND    999999.99</P>
CC DEPOSIT     999      999999.99</P>
CHARGE SALES   999999.99</P>
PAID OUTS      99      99999.99</P>
CARRY OUT SALES 999999.99</P>
CREDIT CARD SALES 999999.99</P>
TAX EXEMPT SALES 999999.99</P>
-----</P>

NET SALES      9999999</P>
OVER/SHORT     9999999</P>
</FORM>
</BODY>
</HTML>
```

FIG.22B

11.a. Transaction Request HTML+D

```
<HTML>
<BODY>
<FORM ACTION=MAIL TO: mail_to>
  ENTER MAIL ADDRESS:
  <INPUT TYPE="TEXT" SIZE=20 NAME=mail_to>
  ENTER MESSAGE:
  <INPUT TYPE="TEXT" SIZE=100>
  <INPUT TYPE="AUTOSUBMIT">
</FORM>
</BODY>
</HTML>
```

FIG.23**FIG.24A****FIG.24B**

1

**OPEN NETWORK SYSTEM FOR I/O
OPERATION INCLUDING A COMMON
GATEWAY INTERFACE AND AN EXTENDED
OPEN NETWORK PROTOCOL WITH NON-
STANDARD I/O DEVICES UTILIZING
DEVICE AND IDENTIFIER FOR
OPERATION TO BE PERFORMED WITH
DEVICE**

This application is a continuation of application Ser. No. 08/995,123 filed Dec. 19, 1997 (now U.S. Pat. No. 5,905,908), which is a continuation of application Ser. No. 08/493,772 filed Jun. 22, 1995 (now U.S. Pat. No. 5,742,845).

FIELD OF THE INVENTION

This invention relates to data transaction systems, and more particularly, to data transaction systems using non-standard input/output devices.

BACKGROUND OF THE INVENTION

Data transaction systems which communicate with a plurality of remote terminals to transfer information used to complete a transaction or compile a database are well known. Typically, such systems include a central transaction processing system which may maintain a database of information such as customer or consumer data. Exemplary information in such a database may include customer identification, customer account numbers, credit limits and/or account balances from which a customer may draw. The central transaction processing system is typically coupled to a plurality of remote transaction or data input terminals. Transaction computers may include special purpose devices such as automatic teller machines (ATMs), point of sale (POS) terminals, credit card terminals, and screen phone terminals. Screen phone terminals are devices which integrate a telephone with an ATM-like device and possibly a magnetic card swipe reader. Data input terminals may include personal computers (PCs) interfaced to data collection devices or special purpose data collection terminals or monitors.

In these known data transaction systems, a user usually initiates a transaction by requesting access to funds in an account or from a credit line maintained by the central processing system. The request is transmitted to the central processing system which performs a verification to determine whether the user is a valid user of the system, has an account within the system, and that the amount of the transaction is within the limits of the consumer's credit line or that the user has the requested funds available in an existing account monitored by the central processing system. The central processing system then transmits authorization for or denial of the transaction to the remote terminal. In response to the message from the central processing system, the remote terminal dispenses cash (for an ATM) or the merchant provides the goods being purchased to the user if the authorization message indicates that the consumer's funds will be transferred to the merchant's account. Similar communication exchanges occur in data systems where electronic documents and other information are provided to a central site for compilation or processing. Consequently, this background discussion applies to all such transaction and data systems. Though the remainder of the discussion is directed to transaction systems, the reader should appreciate that the comments also apply to data systems as well.

The remote terminals may be coupled to the central processing system in several ways. For example, in some

2

ATM systems, the ATMs are coupled to the central processing system through dedicated telephone or other data communication lines. These systems are preferred because they provide a relatively high degree of security since the dedicated data line coupling the central processing system to the ATM is not generally accessible by members of the public. The physical security of the dedicated data line is, however, expensive because no other traffic may utilize the line. Thus, the cost of leasing the dedicated line to an ATM with relatively low volumes of transactions may yield a high communication cost per transaction.

In an effort to reduce the communication cost per transaction, some transaction or data systems utilize telephone lines through a publicly-switched telephone network (PSTN) which may be accessed by other members of the public. Specifically, devices such as credit card terminals and screen phone terminals typically include a modem which converts the digital messages of the remote terminal into frequency modulated analog signals which may be transmitted over telephone lines to a modem at the central processing system. In other systems, the terminal may communicate digital data directly over ISDN lines of the PSTN to the central processing system. This line of communication between a remote terminal and the central processing system is performed by having the remote terminal dial a telephone number associated with the central processing system to establish communication with the central processing system. This type of communication path is relatively secure because the switching networks for the communication traffic through the PSTN are not readily accessible by the public and during the course of the financial transaction, only the central processing system and remote terminal are on the line.

Regardless of the communication method used to couple the central processing system to the remote terminals, the protocol and data formats used between the devices is typically proprietary. That is, the operator of each financial transaction system designs its own protocol and data message format for communication with the processor at the central site or generates a variant within a standard such as those established by the ANSI committee or the like for such communication. As a result, the remote terminals must include software that supports each operator's protocol and message formats in order to be compatible with an operator's central site. For example, application software in a credit terminal such as the TRANZ330, TRANZ380, or OMNI390 manufactured by VeriFone implement one or more of the communication protocols and formats for National Data Corporation (NDC), VISANET, MASTERCARD, BUYPASS, and National Bancard Corporation (NaBANCO) system processors in order to support transactions with the most popular transaction centers. Thus, the communication software absorbs a significant amount of terminal resources which could be used to support other terminal operations.

A related problem arises from the expanding home banking market. A customer of home banking system typically uses a screen phone terminal or a personal computer (PC) having a modem to establish communication through a PSTN to a central transaction processing system. Again, the operator of the central processing system must provide information regarding the data message formats for communicating with the central processing system to a vendor of software for the home banking terminals or must provide that software to its customers. As a result, home banking customers must purchase software to communicate with each banking system of which the customer wants to be a

member. This cost and the need to install additional communication programs may make some consumers reluctant to be a member of more than one banking system or to change banking systems.

A communication system becoming increasingly popular and which provides standardized communication is the Internet. The Internet is an open network of networks which communicate through a variety of physical communication devices such as telephone lines, direct communication lines, and the like. Each network is coupled to the main Internet network for communication through a host computer supporting a TCP/IP router or bridge. The host computer typically includes a program, frequently called a Web server, which acts as a gateway to resources at the host computer which may be resident on the host computer or a network coupled to the host computer. Each server has an address identifying the location of the resources available through the Web server. The router recognizes communication for the server and directs the message to the server or it recognizes that the communication should be forwarded to another server. As a result, communication within the Internet may be point-to-point, but more likely, the communication path is a somewhat circuitous one with the information passing through the routers of multiple servers before reaching its final destination.

A number of message protocols and formats have been developed for the Internet. The physical communication protocol and data message format is the Transport Control Protocol/Internet Protocol (TCP/IP). The TCP/IP protocol involves multiple layers of encapsulating headers containing communication information which are used to provide byte streams or datagram communications to computers on the networks coupled to the Internet. Encapsulated within TCP/IP headers are protocols which are used to format the data messages or transfer data from one computer to another computer coupled to the Internet. These protocols include File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), Telnet, and Hyper Text Transport Protocol (HTTP). The advantage of these protocols is that each provides a standardized communication format for transferring information between computers on the Internet. These protocols are typically called open system protocols as they are publicly known and may be utilized by any programmer to develop programs for communicating with another computer coupled to the Internet. These non-proprietary protocols have contributed to the acceptance of using the Internet as an open network for coupling computer networks together.

While the Internet provides an open network for computer communication with publicly accessible protocols and formats, the Internet suffers from a number of limitations which preclude its effective use as a transaction or data system which uses non-standard I/O terminals and devices. First, circuitous communication presents a number of security issues for such a system. For example, a Web server could incorporate a router which examines the address of each message coming through it and upon recognizing an address associated with a central transaction processing system, copy the data message for the unauthorized retrieval of customer-sensitive information such as account numbers and personal identification numbers (PINs) which may be contained in the message.

A second limitation of open networks such as the Internet is that communication on such networks is only supported for computers acting as servers or clients. Specifically, all of the protocols and formats are constructed for standard input/output (I/O) operations for a PC terminal. That is, text

information is directed to a standard monitor screen, user input is expected from a standard keyboard, and files are transferred to standard peripherals such as a hard disk or diskette drive. Especially absent is the ability in open network protocols for communication with devices that only use communication interfaces such as RS-232C. As a result, communication over the Internet is primarily performed with standard PCs through network communication methods and interfaces.

This presents a number of problems for home banking or for interfacing non-standard I/O terminals such as credit card terminals or screen phones to open networks such as the Internet either directly or through a PC. Generally, non-standard I/O devices are devices which interface to a PC through a port not normally used for networks, such as a RS-232C port, or are devices which have limited input and output capabilities such as small screen displays or ten keypads. These devices are not supported on the Internet because servers use protocols that communicate with PCs supporting standard QWERTY keyboards and standard monitors. Consequently, users are limited to entering account numbers and the like through a keyboard of a PC-like device for processing at a central transaction processing system. To request a transaction, one need only have a person's credit card account number. If the credit card number had to be input through a magnetic card reader, unauthorized access to a customer's account would be less likely since physical possession of the credit card would be required to initiate the transaction.

Another limitation of the standard I/O devices currently supported by the open network protocols is the lack of encryption. For example, PIN pads, which are typically incorporated in ATMs, automatically encrypt in hardware a PIN entered by a user. Such devices typically encrypt the number by implementing a data encryption standard (DES) algorithm in hardware before the PIN is transmitted or stored. When a standard keyboard is used to input the PIN, no hardware encryption is performed and, as a result, an unencrypted copy of the PIN is provided to the memory of the PC. Storage of unencrypted PINs is in contravention of current banking regulations. If PIN pads could be read via Internet protocols, then such a lapse in PIN security would be less likely to occur.

Another I/O device not supported on open networks are smart cards which are increasing in use. Smart cards include a processor and memory in which information regarding the amount of funds in a particular account, a transaction history, account numbers, and customer data may be stored. The card may be read through a smart card reader which is a computer having a processor and memory but usually provided with non-QWERTY keypads and limited displays. A transaction processor may validate a card owner through a PIN provided through a keypad, determine the amount of money remaining on the card and debit the card itself for a transaction amount by communicating with the smart card reader with one of the proprietary protocols discussed above. Such information is not readily obtainable by the owner of the card and so cannot be entered through a keyboard or the like. Smart card readers are non-standard devices which may be coupled to a PC through a COMM1 or COMM2 port. However, none of the standard protocols and message formats for open network communications currently provide I/O operations for such devices.

All systems which attempt to provide three party communication to execute an electronic transaction suffer from a number of limitations which present risks greater than those in a normal transaction performed at the point of sale.

5

In a typical point of sale (POS) transaction, the consumer hands a debit or credit card to a merchant's agent who may examine the card for security markings such as holograms, watermarks, or a cardholder signature. The agent then places the card into a reader for acquiring information from the card and, in some cases, have the consumer enter a PIN into a PIN entry device which encrypts the PIN in a hardware implemented scheme. If the PIN is entered, it is transmitted with the information from the card to a processing center, typically in one of the formats discussed above, under a X.25 protocol or the like. The processing center returns an authorization granted or denied message. The reader typically has a printer coupled to it through an RS-232C port or the like and a purchase agreement is printed. The consumer signs the agreement, the merchant's agent may verify the signature, and the merchant retains an original of the agreement and the consumer a copy. In this scenario, the merchant has initiated the communication to the processing center. The safeguards noted above permit the processing center to charge a merchant a lower processing fee than when a consumer initiates a transaction. Consumer initiated transactions present a greater risk because the consumer provides an agent an account number in a telephone conversation or non-encrypted DTMF transmission. Thus, there is no card inspection, signature verification, or PIN verification. As a result, such transactions are limited to credit cards because debit cards require that the cardholder be present to enter a PIN into an appropriate PIN entry device.

What is needed is a system that permits consumers remote from a merchant to order goods and present payment in a secured manner so the merchant's risk and processing costs, as well as a cardholder's exposure to fraud, is reduced. What is needed is a way for a processing center to communicate through an open network with non-standard I/O devices such as credit card terminals, personal digital assistants, and screen phone terminals or with non-standard I/O devices coupled to the open network through a PC or the like. What is needed is a transaction or data system which utilizes an open network such as the Internet to support electronic transactions or data compilation in a secure manner without undue limitation as to the devices with which communication may be made.

SUMMARY OF THE INVENTION

The present invention provides transaction and data systems which may be implemented on an open network such as the Internet. The system comprises a server for communicating in an open network protocol and a plurality of input/output (I/O) devices coupled to the server through an open network, the I/O devices communicating with the server in the extended open network protocol that supports communication with non-standard I/O devices over the open network. The system of the present invention provides a server with the capability of communicating with a number of I/O devices useful in transaction and data systems which heretofore have been unsupported on an open network system such as the Internet.

The system of the present invention is implemented by extending present open network communication protocols and data message formats to communicate with non-standard I/O devices either coupled to an open network as a client or coupled to an open network through a client, such as a PC, credit card terminal, screen phone, or PDA. That is, commands which are compatible with the communication schema of a presently-implemented protocol for the Internet are used and additions are made to commands implemented within the control structure of that existing protocol to

6

support non-standard I/O device communication. At the server, the extended protocol is further supported by a common gateway interface (CGI) which converts the communication from a non-standard I/O device to a format which is compatible with a transaction or data application program which may be executed on the server or a computer coupled to the server. In this manner, the CGI permits the processing of the extended capability commands to be segregated from the communication functions performed by the server.

Preferably, the server and the I/O devices communicate through an Internet protocol and most preferably, the Hyper Text Transport Protocol (HTTP), to exchange data between an application program and non-standard I/O devices over an open network. Although HTTP is the preferred protocol used to implement the present invention, other protocols such as Telnet or SMTP, for example, may also be extended in a similar manner. Specifically, the HTTP protocol is expanded to communicate with printers, magnetic card readers, credit card terminals, smart card readers, check readers, PIN pads, bar-code readers, PDAs, or the like, and includes a command which instructs a non-standard I/O device to disconnect from the open network and re-couple to a transaction processing system to transfer funds from a consumer account to a merchant account through a PSTN or dedicated data line. By using these extended capability commands within HTTP, a processing system may operate on an open network such as the Internet and communicate with transaction or other data I/O devices which have not previously been able to couple to such open networks. Such a system may be used to execute a transaction between a consumer and a merchant so the merchant receives remittance information in a timely manner. The system permits the consumer to initiate a transaction and order from a merchant and then use a more secure link supported by PIN entry devices or the like to reduce the risk of fraud for the transaction.

Because the server may communicate through such open networks with non-standard I/O devices, the transaction or data processing system is available for the ever-expanding market available through the Internet. Such a system is able to communicate with non-standard I/O devices in myriad locations such as retail establishments or in consumers' homes. For example, a consumer may utilize the standard capability of an Internet protocol to communicate with a server that provides information regarding services or goods for sale over the Internet and then consummate a sales transaction by using the extended capability of the Internet protocol. Such a home consumer could provide transaction data through a smart card reader coupled to a COMM1 or COMM2 port of a PC. A database program executing at the server for the central processing site may accept product ordering information from a non-standard keypad or touch screen associated with a screen phone terminal at the remote site and then communicate with the smart card reader to consummate the transaction. Such a transaction system requires that the consumer have physical possession of the smart or credit card and not simply knowledge of the account number. Likewise, the server would be able to communicate with a PIN pad or the like to ensure the hardware encryption of PINs and other data before it is transmitted to the server site. Such a system is less susceptible to consumer fraud.

Another feature of the present invention is a PAYMENT command implemented in the extended Internet protocol that directs a non-standard I/O device or a PC interfaced with such devices to communicate with a transaction pro-

cessor through an alternative communication link. In one form, the PAYMENT command is used by a merchant terminal to submit a consumer's account number with a merchant deposit account number through a PSTN network or the like to the processing center. In another form of the PAYMENT command, a client program in a consumer's terminal receives an account number for a merchant account from a merchant's server with the PAYMENT command. On receipt of this command, the client program suspends its operation and passes the account number to a conventional bank processing program co-resident in memory. The bank processing program establishes a standard communication link with a transaction processing system through a dedicated data line or a PSTN network. Using that communication link, the bank processing program executes a commercial transaction using a standard VISA protocol or the like. The consumer may use a magnetic stripe reader and a PIN entry device to improve the security of the data transmission. The transaction center may transmit remittance data over the open network to the merchant so the merchant is apprised of payment and ships the ordered product. Once this consumer initiated transaction is complete, the bank processing program terminates and returns control to the client program which may terminate communication with the open network or retrieve information from another server on the open network for another transaction. In this way, the user may use the open network for non-confidential communication such as collecting product information, pricing, and product availability. This information may be collected quickly and efficiently using the extended Internet protocol. The conventional bank processing program and more secure communication links may then be used for the confidential information required for the transaction. Thus, the present invention is able to combine the features and advantages of the Internet with the more secure communication link and data security enhancing devices of systems presently known.

Preferably, an editor is provided which permits a user to define an application database table with data fields, define client application data fields, and define the integrated forms for communicating data between the defined database tables and a client application. The editor verifies the syntax of the user generated integrated forms containing extended Internet protocol statements and client application statements. The editor ensures that the variable names for the client application and the data fields for the database application correspond. Following the generation of the integrated form, the editor parses the integrated form to segregate the database language statements from the extended Internet protocol statements. A database language identifier is substituted in the Internet protocol statements for the database statements contained in the integrated form. The Internet protocol statements are downloaded as a file which is interpreted by the client program for the collection and submission of data from non-standard I/O devices to the database application. The database language statements segregated from the extended Internet protocol statements are placed in a second file which is named to correspond to the database table defined by the user. The CGI application recognizes the database language identifier contained in the returned forms of the Internet protocol statements. The CGI application correlates the database identifier with the file previously generated by the editor which contains the database command statements. The application then inserts the data from the returned form into the database command statements and provides the re-integrated database command statements to the database application. In this manner, the database may be queried by or retrieve data from the non-standard I/O device.

In the most preferred embodiment, the editor permits a user to develop integrated forms comprised of the extended HTML language and standard query language (SQL) database application statements. In this manner, the user does not have to manually generate the SQL commands, the HTML commands, and carefully correlate the data fields of the two commands in order to implement a transaction between a client and a database.

These and other advantages and features of the present invention may be discerned from reviewing the accompanying drawings and the detailed description of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention may take form in various components and arrangement of components and in various steps and arrangement of steps. The drawings are only for purposes of illustrating a preferred embodiment and are not to be construed as limiting the invention.

FIG. 1 is a diagram of an open network system in which the present invention is utilized;

FIG. 2 is a diagram of the format of the FORM and INPUT tags implemented in the preferred embodiment of the present invention;

FIG. 3 is a diagram of the preferred SQL commands supported in the preferred embodiment of the present invention;

FIG. 4 is a flowchart of the high level processing of the client program which interprets the HTML files of the preferred embodiment of the present invention;

FIG. 5 is a flowchart of the HTML file processing performed by the client program of the preferred embodiment of the present invention;

FIG. 6 is a flowchart of the attribute processing for the FORM tag performed by the client program of the preferred embodiment of the present invention;

FIG. 7 is a flowchart of the processing of the ACTION attribute for the FORM tag performed by the client program of the preferred embodiment of the present invention;

FIG. 8 is a flowchart of the processing for the METHOD attribute for the FORM tag performed by the client program of the preferred embodiment of the present invention;

FIG. 9 is a flowchart of the attribute processing for the INPUT tag performed by the client program of the preferred embodiment of the present invention;

FIG. 10 is a flowchart of the processing for the TYPE attribute for the INPUT tag performed by the client program of the preferred embodiment of the present invention;

FIG. 11 is a flowchart of the processing for the NAME attribute of the INPUT tag performed by the client program of the preferred embodiment of the present invention;

FIG. 12 is a diagram of the format for the ACTION attribute for the FORM tag performed by the common gateway interface between the Web server and an application program;

FIG. 13A is a diagram of the possible communication paths which may be used by an I/O device according to the principles of the present invention;

FIG. 13B shows an exemplary FORM tag and INPUT tag for the PAYMENT method implemented in a merchant's terminal according to the principles of the present invention;

FIG. 13C shows an exemplary FORM tag and INPUT tag for the PAYMENT method implemented in a consumer's terminal according to the principles of the present invention;

FIG. 14 shows exemplary integrated statements for a file used in the preferred embodiment of the present invention to

generate the HTML files for the client program and the SQL files for the application program for a card initiated payment authorization and capture transaction;

FIG. 15 shows exemplary integrated statements for a file used in the preferred embodiment of the present invention to generate the HTML files for the client program and the SQL files for the application program for a bar code reader input with card-initiated payment authorization transaction;

FIG. 16 shows exemplary integrated statements for a file used in the preferred embodiment of the present invention to generate the HTML files for the client program and the SQL files for the application program for a key input order with secure payment transaction;

FIG. 17A shows exemplary integrated statements for a file used in the preferred embodiment of the present invention to generate the HTML files for the client program and the SQL files for the application program for a smart card debit (Type 1) transaction;

FIG. 17B shows exemplary integrated statements for a file used in the preferred embodiment of the present invention to generate the HTML files for the client program and the SQL files for the application program for a smart card debit (Type 2) transaction;

FIG. 18 shows exemplary integrated statements for a file used in the preferred embodiment of the present invention to generate the HTML files for the client program and the SQL files for the application program for a debit card transaction;

FIG. 19 shows exemplary integrated statements for a file used in the preferred embodiment of the present invention to generate the HTML files for the client program and the SQL files for the application program for a check verification transaction;

FIG. 20 shows exemplary integrated statements for a file used in the preferred embodiment of the present invention to generate the HTML files for the client program and the SQL files for the application program for a customer frequency transaction;

FIG. 21 shows exemplary integrated statements for a file used in the preferred embodiment of the present invention to generate the HTML files for the client program and the SQL files for the application program for an item search transaction;

FIG. 22 shows exemplary integrated statements for a file used in the preferred embodiment of the present invention to generate the HTML files for the client program and the SQL files for the application program for retail store end of day reporting;

FIG. 23 shows exemplary integrated statements for a file used in the preferred embodiment of the present invention to generate the HTML files for the client program and the SQL files for the application program for a store reporting an e-mail transaction;

FIG. 24A is a diagram of a manual development process for the files interpreted by the client program and the files interpreted by the application program in accordance with the principles of the present invention; and

FIG. 24B is a diagram of the generation of the files interpreted by the client program and the files interpreted by application program performed by an editor constructed in accordance with the principles of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

A transaction or data system constructed in accordance with the principles of the present invention is shown in FIG.

1. The system 10 includes a Web server 12 which is coupled to an open network 14 such as the Internet for communication with various I/O devices and terminals. For example, the I/O devices which may be coupled directly to network 14 include standard I/O devices already supported by Internet protocols such as PCs 30 and non-standard I/O devices such as a screen phone terminal 16, a personal digital assistant (PDA) 18, and a credit card terminal 20. Other exemplary non-standard I/O devices such as smart card reader 32, personal identification number (PIN) pad 34, magnetic card swipe reader 36, printer 38, or the like, may be coupled to PCs through non-standard I/O ports such as COMM1 and COMM2 ports or to other non-standard I/O devices such as phone terminal 16, PDA 18, or credit card terminal 20. Typically, these devices are coupled to PCs or devices 16, 18, or 20 through an interface such as a RS-232C interface. Merchants or other vendors may use a Web server 2 to couple to network 14 to communicate with the devices and processing system 40.

The Web server 12 is preferably coupled to a Common Gateway Interface (CGI) application 28 which converts and communicates the data and commands between the devices on network 14 and the processing system 40 so the I/O devices do not have to use the database command language to interact with the database. System 40 and the devices may communicate directly if they are implemented in the same language or if a user implements a communication interface such as CGI 28 that correlates data fields in the client with those in system 40. Server 12, CGI 28, and the applications supporting system 40 may all reside on a single host computer or they may reside on separate computers coupled together by a local area network (LAN) or a wide area network (WAN). Preferably, the application interfaces with a database which supports Open Data Base Connectivity (ODBC) and Structured Query Language (SQL).

The communication sessions between the I/O devices coupled to the open network 14 and the Web server 12 are generally conducted in the same fashion as Internet protocol communication sessions are currently performed. That is, the I/O device establishes a communication connection with Web server 12, sends a request to the Web server, the Web server responds to the request and the I/O device or server closes the connection. Preferably, the non-standard I/O devices or PCs interfaced to such devices selectively couple to a local access port on the open network 14 through a local modem/ISDN connection. In this manner, the device is only coupled to the open network 14 when a transaction or a data operation is to be performed. While connected to the open network 14, a device may access a number of servers to accomplish a purpose. For example, a device may couple to a local access port and communicate with a first server to check inventory levels at a site, communicate with a second server to order stock for the inventory, and communicate with a third server to settle payment for the ordered goods. When all aspects of the transaction are complete, the connection with the local access port is terminated. In the preferred embodiment of the present invention, the protocol used to transport data messages between Web server 12 and the I/O devices coupled to the open network 14 is the Hyper Text Transport Protocol (HTTP), although other open system protocols utilized on the Internet may be used.

In standard HTTP protocol, a client program executing in one of the I/O devices may initiate communication with a server by sending a query message of the format:

http://<host>:<port>/<path>?<search part>

The message identifies the client as seeking communication with a HTTP server at the host address on the specified

port. In the HTTP protocol, the default value for the port is 80 and the host address is the Internet protocol (IP) address of the type well-known in the art. The path value selects the file in the HTTP server which is activated in response to the message and the search part specifies a query for the selected file. In the initial communication, the query may be omitted so that the selected host file responds to the client program before a query is processed.

In the present invention, the client program uses a similar message to initiate a transaction or data operation, except that database commands are preferably embedded in a file at the server 12 and not in the "search part" of the command, although search parts may be constructed in accordance with the principles of the present invention that support non-standard I/O devices. Preferably, the client program interprets Hyper Text Markup Language (HTML) files containing HTML commands for communicating data between non-standard I/O devices and server 12. Most preferably, the HTML commands contain identifiers which are used by the CGI to place data returned in the forms of the HTML commands into database commands for queries or data insertions for the database. HTML is a command language well known for the retrieval and display of electronic documents for standard I/O devices such as PCs supported by full screen monitors, QWERTY keyboards, and standard peripherals such as hard disk drives and diskette drives. Standard HTML commands use text and previously known commands that reference Universal Resource Locators (URLs) to support the communication of electronic documents. These documents are files which may contain HTML commands, text, audio, video, or image data. The present invention extends HTML with commands that support communication between the server and the non-standard I/O devices.

In the HTTP protocol, data may be obtained during a communication session by using a tag called a FORM as part of the file defined by <path> in the command discussed above. The FORM format for standard HTTP is:

```

<FORM ACTION="URL"
  METHOD=GET POST
>
  Command
</FORM>

```

where "|" is an "OR" operator. The commands supported by standard HTTP are INPUT, SELECT, and TEXTAREA. Additionally, standard HTTP permits the inclusion of text data in the command area. In the present invention, HTML has been extended to support new ACTIONS, METHODS, and INPUTs.

In accordance with the principles of the present invention, tags are preferably used to identify device transfers and input operations. Preferably, the FORM tag is used to identify device transfers and ACTION and METHOD attributes further identify the device operation. As shown in FIG. 2, the extended ACTION field may include a FROM and TO attribute for accessing a local terminal file or smart card reader or a TO PRINTER attribute for directing output data to a printer local to the I/O device. The FROM and TO attributes for accessing local files and smart card readers and for directing output data to a local printer have previously been unsupported in any Internet protocol. As a result, the server 12 may access non-standard I/O peripherals for any of the I/O devices used in the transaction or data system 10. The ACTION="URL" is a part of standard HTTP and is well known.

The METHOD attributes may include the GET, POST, PAYMENT, or SQL methods. The GET and POST methods are currently supported in standard HTTP and are well known. The PAYMENT attribute is a directive to deliver data retrieved by an INPUT command to a private payment network for authorization and settlement and is not available in current Internet protocols. This directive is used by the client program to activate a conventional financial transaction application which communicates with the transaction system over a dedicated data line or PSTN in a known protocol such as VISA. Such an attribute is used where the more secure physical connection between remote site and transaction system and data encryption devices or the like are preferred. The SQL method preferably identifies a database language file which CGI 28 uses to correlate data in the HTML FORM to an insertion or query command contained in the file.

The preferred format for the INPUT tag which is used to identify input operations is also shown in FIG. 2. The TYPE and NAME attributes are used to define a non-standard I/O device or local storage variable for the input of data. The TYPE field values "text," "password," "checkbox," "radio," "submit," and "reset" are previously known, as are the attributes NAME, VALUE, CHECKED, SIZE, and MAX-LENGTH. To support the extended capability of the present invention, the TYPE attribute preferably includes attributes MSRT1 for reading track 1 of a magnetic swipe reader, MSRT2 for reading a magnetic swipe reader track 2, KEY for reading input from a terminal command keypad, PIN for reading a personal identification number pad, BCW for reading a bar code wand, MICR for reading a check magnetic code reader, ATM for reading a dollar amount via a key input mask, INT for reading an integer via a key input mask, LOCAL for reading input from a variable in the local storage of an I/O device, and AUTOSUBMIT for returning a FORM with information to the server.

The NAME attribute used with the INPUT tag identifies reserved word names for local storage in the device executing the client program. Preferably, the NAME attribute identifies ip_address, host_phone, tid, work_key, datetime, and deposit_acct as local storage areas in the local device for the terminal's Internet Protocol (IP) address, Internet access phone number, terminal ID, PIN encryption working key, date/time, and merchant account number, respectively. These attributes are used with the INPUT tag to read non-standard I/O devices which may be coupled to open network 14. For example, an INPUT TYPE=MSRT1 attribute causes the client program residing within a magnetic stripe reader to input data from track 1 of a stripe reader and insert that data into a FORM which is returned to Web server 12 for processing by an INPUT TYPE=AUTOSUBMIT statement.

Preferably, the database language commands which may be embedded in the extended HTML are SQL commands such as those shown in FIG. 3, although other database languages may be used. The SELECT command may include the names of data fields in a database so the device on network 14 may request a data item from a database at the central processing system. The database table is identified by the FROM attribute and the conditional selection of data from an identified database table may be defined by a WHERE attribute. Additionally, records may be requested from an identified database in ascending or descending order or in groups of two records at a time using the ORDER attribute. Additionally, the SELECT field command with the GROUP attribute provides I/O devices with the capability of retrieving records grouped under an identified name.

13

Additionally, the I/O devices may either insert new data into an identified database with the INSERT attribute or update data already existing in a database with the UPDATE attribute. The values for the INSERT attribute may be identified with the VALUES attribute, and the SET and WHERE attributes may be used to define and conditionally update values in the identified database. Preferably, the present invention implements two DELETE and CREATE attributes. The DELETE attribute deletes all items in an identified column of a database table which may satisfy a condition defined by a WHERE attribute. The CREATE attribute creates a database table having a primary key identified by the PRIMARY KEY attribute.

Preferably, the server program executes on a computer system having at least an Intel 80386 or better processor with at least 4 megabytes of RAM and at least 3 megabytes of hard disk space available. The computer system running the server may operate any known server platform operating system such as WINDOWS 3.1, WINDOWS 95, or WINDOWS NT, UNIX, AIX, and others. The non-standard I/O devices require a processor of a Z80A type or better, at least 32K bytes of RAM, and at least 32K bytes of ROM. The device includes a modem capable of at least 1200 bits-per-second (bps) but other modem speeds may be used for communication between client and server. Alternatively, the device may be coupled to a LAN which in turn is coupled to the Internet for communication with server 12. A typical non-standard device which executes the client program is a VeriFone OMNI390, OMNI395, or VuFone terminal. OMNI390, OMNI395, and VuFone are trademarks of VeriFone, Inc., of Redwood City, Calif. Other exemplary devices include Phillips Screen phone, Hypercomm T7 terminal, and Apple Computer Newton MessagePad.

To build the preferred HTML files which CGI 28 preferably uses to implement the client program and database application, the user preferably uses an off-line editor. The files generated by the editor are preferably comprised of an integrated statements formed from HTML statements and database statements for retrieving and writing data with the database. Exemplary files showing such integrated statements for performing transactions are depicted in FIGS. 14-23B. After such a file is generated, the editor parses the integrated statements into HTML statements and into database statements such as SQL commands. The HTML files required by the client program to support communication with a transaction or data processing center may be downloaded to a device or PC for execution. The files containing the database application statements used by the CGI interface to communicate data with the database application program preferably reside on server 12. Preferably, the database files used by the CGI interface include SQL commands for the application program interfaced to an ODBC compliant database.

The general format of the HTML commands in the HTML files used for communication with a client program and server are of the general format: TAG ATTRIBUTE. Preferably, the TAG field may be one of FORM, INPUT, SQL, or TEXTAREA. The ATTRIBUTE field value depends upon the TAG value. Preferably, the FORM tag may include the ACTION or METHOD attributes where the ACTION attributes include the FROM<file>, TO PRINTER, TO<file>, and TO SCR values noted above, as well as the standard HTML ACTION value of URL=<file>. The METHOD attributes include the PAYMENT and SQL attributes noted above, as well as the standard HTML METHOD values of GET and POST. Also in accordance with the principles of the present invention, the INPUT tag

14

may include TYPE, NAME, VALUE, CHECKED, SIZE, and MAXLENGTH attributes. These attributes are previously supported for the INPUT tag in HTML, however, the present invention further includes TYPE values of MSRT1, MSRT2, KEY, PIN, BCW, MICR, AMT, INT, LOCAL, and AUTOSUB, as well as the standard HTML TYPE values of TEXT, PASSWORD, CHECKBOX, RADIO BUTTON, SUBMIT, and RESET. The present invention also supports NAME attributes of IP_ADDRESS, HOST_PHONE, TID, WORK_KEY, DATETIME, and DEPOSIT_ACCT to identify local storage areas as well as standard HTML NAME attribute <Field_NM> to identify a FORM variable.

The preferred high level processing of the client program is shown in FIG. 4. That processing includes an idle step (Block 100) in which the program performs general house-keeping tasks such as maintaining internal time, scanning for input which may activate the device, or other known functions. Further processing is activated by some operator action at the device or PC which causes the device to either open a remote URL (Block 102) or open a local URL (Block 104). If a remote URL is required, the device transmits a message of the format discussed previously which is routed through the open network and delivered to a server 12 for a transaction or data processing system (Block 106). The HTML file selected at the server 12 is identified by the remote URL in the initial communication between the device and server 12 and that URL is used to return the selected HTML file to the device for processing (Blocks 108, 110).

FIG. 4 also shows that an operator may initiate an open local URL function by typing in a command or by pushing a hot key which is associated with a local URL. The I/O device reads the HTML file identified by the URL from local memory (Block 112) and passes the HTML file to the function for processing HTML files (Block 110). After a file is processed (Block 110), the client program determines whether the HTML file is to be stored (Block 114). If it is not, the process returns to the idle processing (Block 100). Otherwise, the process determines whether the HTML file is to be associated with a hot key (Block 116) and, if it is, stores the file and generates the link between a hot key and the stored file (Blocks 118, 120). If the HTML file is only to be stored, no association is made with a hot key and the file is simply stored in local memory (Block 20). The client program then returns to idle processing (Block 100).

The high-level processing for the HTML file (Block 110, FIG. 4) is shown in further detail in FIG. 5. The process begins by scanning the HTML file for a TAG (Block 140). If no TAG is found, the file is not in proper format for processing and processing returns to Block 114 discussed in FIG. 4 above. If a TAG is found (Block 142), the process determines whether the TAG is a FORM TAG (Block 144) or an INPUT TAG (Block 146). If it is a FORM TAG, then the FORM TAG is processed and the program continues by looking for other TAGS to process (Block 140). If the TAG is an INPUT TAG, the INPUT TAG is processed (Block 150) and the program continues by looking for other TAGS to process (Block 140). If the TAG is one of the standard HTML TAGS, the program implements the TAG in standard known ways (Block 152) and then scans for other TAGS to process (Block 140).

Processing the ATTRIBUTES used to implement a FORM TAG is shown in FIG. 6. That process continues by scanning the HTML file for an attribute (Block 160). If an attribute is not found (Block 162), the program returns to scan for other TAGS (Block 140, FIG. 5). If an attribute is found, the program determines whether it is an ACTION

15

attribute (Block 164) or a METHOD attribute (Block 166). Depending on the type of attribute, the appropriate function for processing the attribute is executed (Blocks 168 or 170) and scanning for additional attributes continues (Block 160). If the attribute is not an ACTION or METHOD attribute, there is an error in the file and processing returns to scan for other TAGs.

The processing for the ACTION attribute is shown in FIG. 7. There, the ACTION attribute is examined to determine whether it is a FROM<file> (Block 180), TO PRINTER (Block 182), TO<file> (Block 184), TO SCR (Block 186), FROM SCR (Block 188) or a URL=<file> (Block 192). The URL=<file> ACTION is a standard HTML action which is processed in a known way (Block 194). The FROM <file> action is processed by reading data from a file associated with the I/O device or PC interfaced to the I/O device (Block 196). The TO PRINTER action results in data in the FORM being sent to the printer (Block 198) while the TO <file> action results in data in the FORM being written to a local file (Block 200). The TO SCR action causes data to be written to the smart card via a smart card reader (Block 202) and the FROM SCR reads data from a smart card through a smart card reader (Block 204). After the appropriate action processing takes place, the HTML file is scanned for additional ACTION values to perform (Block 206), and if one is found, the process continues. If no attribute is located (Block 208), the process returns to scan for other attributes (Block 160, FIG. 6).

The processing for the METHOD attributes for FORM tags are shown in FIG. 8. The process determines which type of METHOD is present in the FORM and then properly processes the attribute. For the GET and POST methods (Blocks 210, 212) the processing is the same as that performed in standard HTML (Blocks 226, 228). That is, for the GET method, the identified URL<file> is queried for data while the POST attribute causes data to be transferred to the URL<file>. The preferred METHOD attributes extending the HTML implementation of the present invention are SQL (Block 214), and PAYMENT (Block 224) attributes. The SQL attribute is preferably not expanded into a SQL command at the client, but rather is expanded by the CGI 28 at server 12 by correlating the data or variable field names in a returned form with the SQL commands stored at the server. This processing is done in a manner described in more detail below. The client program passes the SQL file identifier to the server 12 (Block 230). The processing of the PAYMENT command (Block 232) is discussed in more detail below. The HTML file is scanned for other METHODS (Block 242, 244), and, if one is found, the processing continues by identifying the METHOD (Blocks 210-224). Otherwise (Block 244), the process returns to scan the HTML file for other ACTION or METHOD attributes (Block 160, FIG. 6).

Processing for the INPUT tag is shown in FIG. 9. The process scans the HTML file following the INPUT tag for attributes (Block 250). If no attributes are found (Block 252), the process continues by scanning the HTML file for other tags to process (Block 140, FIG. 5). If an attribute is found and it is a TYPE attribute (Block 254), it is processed (Block 256), and if the attribute is a NAME attribute (Block 258), it is processed (Block 260). Both the TYPE and NAME processing is shown in more detail in FIGS. 10 and 11, respectively. If the attribute is neither a NAME or TYPE attribute, it is a standard attribute for an INPUT tag supported by standard HTML and is processed in a known manner (Block 262). Following processing of the INPUT attribute, the HTML file is scanned for other attributes to process (Block 250).

16

Processing for the TYPE attribute is shown in FIG. 10. The process first identifies the TYPE attribute for the INPUT tag and then performs the appropriate processing. The new TYPE attributes of the preferred embodiment of the present invention are MSRT1 (Block 270), MSRT2 (Block 272), KEY (Block 274), PIN (Block 276), BCW (Block 278), MICR (Block 280), AMT (Block 282), INT (Block 284), LOCAL (Block 286), and AUTOSUB (Block 288). If the TYPE attribute is not one of these, it is a standard HTML type attribute that is processed in a known manner (Block 310). Each of the new HTML TYPES supported by the present invention causes an I/O operation with a non-standard device. Specifically, these operations are the reading of Track 1 of the magnetic stripe reader (Block 290), the reading of the second track of the magnetic stripe reader (Block 292), the reading of a keypad (Block 294), the reading of an encrypted PIN through a PIN entry device (Block 296), the reading of a bar code through a bar code reader (Block 298), the reading of encoded data on a check through a magnetic check reader (Block 300), the reading of a dollar amount from a keypad through a key input mask (Block 302), the reading of a number from a keypad through a key input mask (Block 304), the reading of data from a local variable (Block 306) and the submission of the data read from one of these devices in a FORM returned to the server 12 (Block 308). The data mask for AMT constrains the dollar amount read to a predetermined number of characters with only two characters following the decimal point. The data mask for INT ensures the number is an integer value within a predetermined range. Processing continues by scanning the HTML file for other TYPE attributes (Block 312) and, if another TYPE attribute is found (Block 314), processing continues by determining the TYPE attribute and performing the appropriate processing. Otherwise, the process returns to scan the HTML file for other attributes (Block 250, FIG. 9).

The NAME attribute processing is performed in accordance with the process shown in FIG. 11. That process examines the NAME attribute to determine if the variable name identified by the attribute is IP_ADDRESS, HOST_PHONE, TID, WORK_KEY, DATETIME, or DEPOSIT_ACCT (Blocks 320, 322, 324, 326, 328, 330). If they are, the INPUT value resulting from one of the INPUTS in a FORM of the HTML file is stored in a local variable identified by the NAME attribute. Following storage (Block 332), the file is scanned for other NAME attributes (Block 328) and, if there are none (Block 332), processing continues by scanning for other attributes for the INPUT tag (Block 250, FIG. 9). If the NAME attribute is a standard HTML INPUT NAME, it is processed by known methods (Block 336). Processing then continues by scanning for other NAME attributes to process (Block 338, 340). Otherwise, the process returns to scan the HTML file for other attributes (Block 250, FIG. 9).

CGI 28 receives Internet protocol statements in a file transmitted from a client program and provides data from those statements to the application(s) implementing system 40 and receives the output of system 40 and provides them to the client program in a file. CGI 28 may be implemented by a program developed by a user using a manual development method as shown in FIG. 24A. That method requires a user to generate a system definition from which a file statement definition for the client and application are developed to implement the transactional or data system. Using the file statement definitions, the user generates the files for the client and database programs which are interpreted by the respective programs to implement transactions or data

17

processing. This process requires the user to not only have knowledge regarding the transaction or data process but specific details of the interaction between the client and database. The user is further required to resolve and correlate all data identifiers in the statements for the client and database environments.

Preferably, CGI 28 is developed with an editor that only requires the user to define the system with statements which are an integration of the protocol statements and the database language. The process implemented by this editor is shown in FIG. 24B. Examples of such integrated statements for files which implement a specific transaction are shown in FIGS. 14 to 23B. The editor verifies the syntax of the integrated statements and correlates the data variables of the protocol statements with the data fields of the database. Following the generation of the integrated statements, the editor segregates the protocol statements from the database language statements. The protocol statements are stored in files which are identified as being for a particular transaction or data process and the database statements are stored in files which are identified as being for a particular transaction or data process on an identified database table. The editor places a database file identifier in the protocol statements which contained embedded database statements. The database file identifiers are used by CGI 28 to select the file for the appropriate transaction so CGI 28 may correlate data variables in the protocol statements with data fields in the database files. The files containing statements to be interpreted by the client program are then downloaded to the appropriate terminals, and the database files containing database language statements are stored on the system executing the CGI 28.

Alternatively, the editor of the present invention may parse integrated statements which are segregated into source code statements for first and second processors, such as an editor further includes a compiler to generate executable code for each processor and, if the processors execute differing source code, a compiler for each source code language. The executable code may then be downloaded to the respective processors for execution.

More specifically, the editor preferably places the database statements for one of the transactions of the preferred embodiment in a file identified by the database name following SQL in FIG. 12. The attributes and tags forming the HTML statements for one of the transactions of the preferred embodiment are placed in a file generally denoted as <html_file>.HTM. The name <html_file> is a name which identifies one of the transactions. Where SQL statements are in the fields of the integrated statements shown in FIGS. 14 to 23B, the string "<html_file>.SQL" is substituted as the database name in the statements of the <html_file>.HTM file. When the CGI executable file is initiated and parses the returning forms, the returned data is placed in the corresponding "<html_file>.SQL" file which is passed to the application program as a command line argument. In this manner, an abbreviated form for the SQL commands may be communicated over the open network between the client and CGI and the CGI may be able to expand those abbreviated SQL commands into the appropriate SQL commands which the application program requires to manipulate the ODBC database.

To effectuate a transaction, for example, an operation at a terminal with non-standard I/O devices may activate a terminal file with a hot key or other action. In processing the activated file, the client program may acquire data which is stored in a local variable or accessible through a non-standard I/O device. This data may then be stored in a

18

FORM and submitted to a server file at a processing system address. The server file activates CGI 28 which retrieves data from the FORM and incorporates it into database statements in the database file for the appropriate transaction and database. If the database statement is a query, the requested data is returned to the CGI in the database file and the CGI places it in the corresponding FORM variables so the server may return the data to the terminal. If the database statement provides data to a database to obtain an authorization, for example, the action performed by the database application in response to the data is placed in the corresponding FORM and returned to the terminal. In this way, data is exchanged between the terminal and the database application. This exchange is supported by CGI 28 even though the server/client communication is performed in an open system protocol, such as HTTP, and the database application is performed in another language, such as SQL. CGI 28 is able to convert and exchange the data between the client and database without the user having to specifically design and implement a conversion program.

The communication paths available for a device implementing the present invention are shown in FIG. 13A. As shown there, an I/O device 420 is coupled through the WorldWide Web open network 426 to an Internet Web server 12. This connection may be implemented with the preferred extended capability HTML described above. Although HTML files may be encrypted to enhance the security of the document as it is communicated across the Internet, the operator of the system may choose to utilize a more secure physical connection between the device 420 and the Web server 12. To obtain this alternative connection, the PAYMENT command for the METHOD attribute is preferably used. One form of the PAYMENT command is for a merchant's terminal and the other is for a consumer's terminal. In either terminal, the client program which supports the extended capability HTML operates independently but co-resident in memory with a certified bank card authorization and capture application, which may be provided by a financial institution or a bank card processor.

For the form of the command shown in FIG. 13B, the client program in the merchant terminal suspends its execution and passes the terminal identifier, stored locally, which identifies the merchant's account and the consumer account information read via a magnetic stripe reader or the like, to the bank card application. The bank card application communicates this information via a PSTN 424 or the like to a transaction processor 422. The processor 422 authorizes or denies the transaction and, if authorized, a printer at the merchant terminal prints a purchase agreement which the consumer may execute to complete the transaction.

In response to a HTML file having a FORM with an ACTION attribute equal to an executable file name for a bank card application program or the like, a METHOD attribute with a field value of PAYMENT, and an INPUT tag with a TYPE attribute of LOCAL_NAME which identifies a deposit only account supplied by a merchant (as shown in FIG. 13C), the client program is suspended and control is transferred to the bank processing application. The bank processing application then uses a modem or ISDN D channel using T3 POS protocol or the like to connect to a secure packet network 424 to connect in a virtual point-to-point manner with a payment processor through a PSTN network or the like. This physical connection provides an additional security element to the encrypted data for the transaction of account information, PIN numbers encrypted by PIN pads provided at the consumer site, and other sensitive information. The bank processor 422 may submit

19

remittance data to the merchant, via the Web or otherwise. After receiving the remittance data, the merchant may ship the product to the consumer. Thus, in this manner, the I/O device may communicate with a plurality of Web servers to "shop" for a best price, delivery date, or other relevant information for selecting a preferred transaction, and then execute the PAYMENT method to utilize a more secure physical communication connection and data security devices to consummate the financial elements of the transaction with less risk and costs for the merchant, consumer, and bank processor.

The preferred integrated HTML/SQL statements which support a card initiated payment authorization and capture transaction are shown in FIG. 14. A first file 500 includes statements which identify the URL database from which the non-standard I/O device seeks authorization for a transaction. The prompts to the operator to enter the account number and amount of the transaction are supported by the INPUT tags which read the second track of the magnetic stripe reader to accept a number of up to 40 characters and assign that information from that track to a variable, and to input the up to 8 characters from the keyboard or the like into a variable called AMOUNT. The INPUT tag with the TYPE attribute of AUTOSUBMIT returns the form to the server for processing in accordance with the method defined in the returned form. As shown in FIG. 14, that METHOD statement causes CGI 28 to incorporate returned data into SQL commands which query the database as to whether the subfield of the track 2 data representing the account number is present in the authorization table of the database. If the data is not present, then a new record is inserted into a table labeled "log_table". The new record consists of the account number and the amount returned in the FORM. Based upon the results of this processing, the application program supplies the data fields to the FORM which will be returned to the client program for printing the transaction record. That file 510 is shown in FIG. 14. The ACTION attribute TO PRINTER and the POST METHOD causes the data in the next eight lines to be directed to the printer coupled to the non-standard I/O device for printing the transaction form. The customer may then execute the printed form to complete the transaction. If the transaction is declined or an error is otherwise encountered, the file 520 is used to return a denial to the client program.

In a similar manner, the preferred integrated statements for a bar code order input with card-initiated payment authorization is shown in FIG. 15. The file 550, supported by the present invention which implements the transaction request, is again directed to the proper database by the ACTION attribute. The necessary customer information such as name and address may be input through a standard keyboard. The HTML command in the present invention also permits the form to receive the bar code, unit price, and credit card information in a manner similar to that discussed above for the magnetic card reader. Once this information is returned to the server and CGI interface, it is processed by the application program in accordance with the METHOD identified in the returned form. The method of HTML file 550 also creates a database order_table having the information shown in the method. Again, if the transaction is approved, the data for the order and customer acceptance of the order is provided in HTML file 555, which is directed by the ACTION attribute to the printer at the non-standard I/O device. If the account number is not in the authorization database, the authorization declined or error response is provided in correspondence with the statements in file 560.

In a similar manner, FIGS. 16-22 show the integrated statements for a transaction request, authorization response,

20

or authorization declined response files for key input order with secure payment transaction (FIG. 16), a smart card-debit (Type 1) transaction (FIG. 17A), a smart card debit (Type 2) transaction (FIG. 17B), a debit card transaction (FIG. 18), a check verification transaction (FIG. 19), a customer frequency transaction (FIG. 20), an item search transaction for which there is no denial (FIG. 21), retail store end of day reporting (FIG. 22) and a store reporting an e-mail transaction (FIG. 23).

While the present invention has been illustrated by the description of a preferred and alternative embodiments and processes, and while the preferred and alternative embodiments and processes have been described in considerable detail, it is not the intention of the applicant to restrict or in any way limit the scope of the appended claims to such detail. Additional advantages and modifications will readily appear to those skilled in the art. For example, rather than expanding HTTP to support non-standard I/O devices, the FTP, POP, SMTP, TELNET or other protocols may be expanded in like manner to couple non-standard I/O devices to the Internet. Similarly, the preferred implementation of the present invention supports a variety of non-standard I/O devices and I/O operations. An Internet protocol may be constructed in accordance with the principles of the present invention to support only selected I/O devices or operations disclosed in the present application. The invention in its broadest aspects is therefore not limited to the specific details, preferred embodiment, and illustrative examples shown and described. Accordingly, departures may be made from such details without departing from the spirit or scope of applicant's general inventive concept.

What is claimed is:

1. A method for communicating between a client program controlling in a non-standard input/output (I/O) device and a server over an open network comprising:
 - activating a non-standard I/O device to assign data obtained by a non-standard I/O device to a variable name in a file comprised of extended open network protocol statements; and
 - sending a file having said assigned data to a server to perform a data operation in accordance with said extended open network protocol statements.
2. The method of claim 1 further comprising:
 - identifying in one of said extended open network protocol statements an I/O operation for said non-standard I/O device to obtain said data for said assignment.
3. The method of claim 1 further comprising:
 - identifying a processing method for said data operation with said assigned data.
4. The method of claim 1 further comprising:
 - receiving a file comprised of extended open network protocol statements generated by said server from said data operation; and
 - performing a data operation with said non-standard I/O device in accordance with at least one of said generated extended open network protocol statements in said received file.
5. The method of claim 4 wherein said data operation is performed by executing an executable file identified by one of said generated extended open network protocol statements in said received file.
6. A method for communicating between a client program controlling a non-standard input/output (I/O) device and a server over an open network comprising:
 - generating a file comprising extended open network protocol statements, at least one of which identifies a data operation for obtaining data from a non-standard I/O device; and

21

sending said file to a client program controlling said non-standard I/O device.

7. The method of claim 6 further comprising:

receiving data obtained by said non-standard I/O device performing said identified data operation. 5

8. The method of claim 7 further comprising:

performing a data operation with said data received from said non-standard I/O device;

generating extended open network protocol statements from said data operation; and 10

sending a file comprising said generated extended open network protocol statements to a client program controlling said non-standard I/O device. 15

9. The method of claim 8 wherein said data operation identification is achieved by identifying an executable file name in one of said extended open network protocol statements. 20

10. A system for communicating between a client program controlling a non-standard input/output (I/O) device and a server over an open network comprising:

means for activating a non-standard I/O device to assign data obtained by a non-standard I/O device to a variable name in a file comprising extended open network protocol statements; and 25

means for sending a file having said assigned data to a server to perform a data operation. 30

11. The system of claim 10 further comprising:

means for identifying in one of said extended open network protocol statements an I/O operation for said non-standard I/O device to obtain said data for said assignment. 35

12. The system of claim 11 further comprising:

means for identifying a processing method for said data operation with said assigned data.

22

13. The system of claim 11 further comprising:

means for receiving a file comprising extended open network protocol statements generated by said server from said data operation; and

means for performing a data operation at said non-standard I/O device in accordance with at least one of said generated extended open network protocol statements in said received file.

14. The system of claim 13 further comprising:

an executable file for performing said data operation, said executable file being identified by one of said generated extended open network protocol statements in said received file.

15. A system for communicating between a client program controlling a non-standard input/output (I/O) device and a server over an open network comprising:

means for generating a file comprising extended open network protocol statements, at least one of which identifies a data operation for obtaining data from said non-standard I/O device; and

means for sending said file to a client program controlling said non-standard I/O device.

16. The system of claim 15 further comprising:

means for receiving data obtained by said non-standard I/O device performing said data operation.

17. The system of claim 16 further comprising:

means for performing a data operation with said data received from non-standard I/O device;

means for generating extended open network protocol statements from said data operation; and

means for sending a file comprising said generated extended open network protocol statements to a client program controlling said non-standard I/O device.

18. The system of claim 17 wherein said means for performing a data operation is an executable file.

* * * * *